

FIG. 1

4. 3 - 2 -

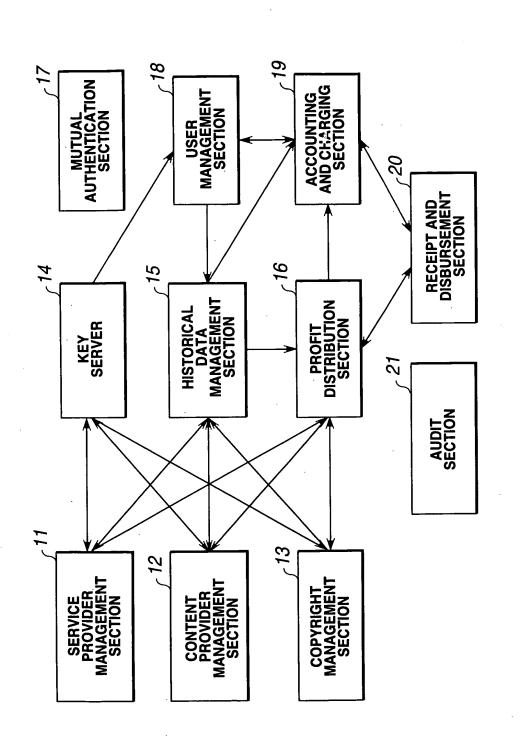


FIG.2

1998/2/28

1998/1/31

1998/1/1

aaaaaaaa bbbbbbbb ccccccc

START

VERSION OF DISTRIBUTION KEY

DISTRIBUTION

**AVAILABLE PERIOD** 

1998/3/1 1998/3/31

				=				3/88	
CE CENTER	AVAILABLE PERIOD START END	1998/1/31	1998/2/28	1998/3/31	1998/4/30	1998/5/31	1998/6/30		EIVER
EMD SERVI	AVAILABL START	1)1988/1/1	1998/2/1	1998/3/1	1998/4/1	1998/5/1	1998/6/1	NOIT	LD BY RECI
DISTRIBUTION KEYS HELD BY EMD SERVICE CENTER	VERSION OF DISTRIBUTION KEY	1	2	3	4	2	9	TRANSMIT DISTRIBUTION KEY	DISTRIBUTION KEYS HELD BY RECEIVER
TRIBUTION KI	DISTRIBUTION KEY	aaaaaaa	qqqqqqqq	ວວວວວວວ	ppppppppp	eeeeeee	ffffffff	·	DISTRIBUT
		DISTRIBUTION KEY TO BE LISED			_	TDANCMIT	DISTRIBUTION	NEW CONTRACTOR OF THE PROPERTY	-
CONTENTS PROVIDER	AVAILABLE PERIOD	1998/1/31	1998/2/28	1998/3/31	1998/4/30	1998/5/31	1998/6/30		
_	AVAILABI START	1/1/8661	1998/2/1	1998/3/1	1998/4/1	1998/5/1	1998/6/1		
KEYS HELD B	VERSION OF DISTRIBUTION KEY	-	2	က	4	2	9	·	
DISTRIBUTION KEYS HELD BY	DISTRIBUTION	aaaaaaaa	qqqqqqqq	ວວວວວວວ	ppppppppp	өөөөөөөө	fffffff		-
_		NON PER	3						

**-1G.3** 

1998/2/1 | 1998/2/28

qqqqqqqq

START

DISTRIBUTION DISTRIBUTION KEY KEY

**AVAILABLE PERIOD** 

1998/3/1 1998/3/31 1998/4/1 1998/4/30

pppppppp

										77 JU	
CE CENTER	E PERIOD	END	1998/1/31	1998/2/28	1998/3/31	1998/4/30	1998/5/31	1998/6/30	1998/7/31		EIVER
EMD SERVI	AVAILABLE PERIOD	START	1998/1/1	1998/2/1	1998/3/1	1998/4/1	1998/5/1	1998/6/1	1998/7/1	SMITUNOTTON	LD BY REC
EYS HELD BY	VERSION OF	KEY	1	2	3	4	5	9	7	TRANSMIT DISTRIBUTION KEY	DISTRIBUTION KEYS HELD BY RECEIVER
DISTRIBUTION KEYS HELD BY EMD SERVICE CENTER	DISTRIBUTION	KEY	aaaaaaa	qqqqqqq	၁၁၁၁၁၁၁	pppppppp	<b>өөөөөөө</b>	fffffff	99999999		DISTRIBUT
			DISTRIBUTION KEY TO BE LISED			•	THANGU	DISTRIBUTION	KEY	7	
BY CONTENTS PROVIDER	AVAILABLE PERIOD	S	1998/2/28	1998/3/31	1998/4/30	1998/5/31	1998/6/30	1998/7/31			
3Y CONTEN	AVAILABI	START	1998/2/1	1998/3/1	1998/4/1	1998/5/1	1998/6/1	1998/7/1			
_	VERSION OF	DISTRIBUTION	2	3	4	2	9	7			
DISTRIBUTION KEYS HELD	NOITIBIBILITION	KEY	qqqqqqq	2222222	pppppppp	eeeeeee	ffffffff	9999999			
			SUTION	3E USED							

FIG.4

1998/4/1 | 1998/4/30 1998/3/1 | 1998/3/31

**AVAILABLE PERIOD** 

DISTRIBUTION KEYS HELD BY RECEIVER

EN S

START

က

၁၁၁၁၁၁၁ ppppppppp eeeeeee

VERSION OF DISTRIBUTION KEY

DISTRIBUTION

1998/5/1 | 1998/5/31

Ŋ

										5.	/81
CE CENTER	E PERIOD	END	1998/1/31	1998/2/28	1998/3/31	1998/4/30	1998/5/31	1998/6/30	1998/7/31	1998/8/31	
EMD SERVI	AVAILABLE PERIOD	START	1998/1/1	1998/2/1	1998/3/1	1998/4/1	1998/5/1	1/9/8661	1/2/8661	1998/8/1	
DISTRIBUTION KEYS HELD BY EMD SERVICE CENTER	VERSION OF	KEY	1	2	3	4	2	9	7	8	
TRIBUTION KE	DISTRIBUTION	KEY	aaaaaaa	qqqqqqqq	ງວວວວວວ	ppppppppp	99999999	ffffffff	99999999	hhhhhhhh	
			DISTRIBUTION aaaaaaaa	NET TO DE COED		•	TIMORES	DISTRIBUTION	KEY	7	
<b>IS PROVIDEF</b>	AVAILABLE PERIOD	ENO	1998/3/31	T	1998/5/31	1998/6/30	1998/7/31	1998/8/31			
Y CONTEN	1	0,	1998/3/1	1998/4/1	1998/5/1	1998/6/1	1998/7/1	1998/8/1			
KEYS HELD B	VERSION OF	DISTRIBUTION DISTRIBUTION KEY	8	4	5	g	7	. 00			
DISTRIBUTION KEYS HELD BY CONTENTS PROVIDER		NSI KIBO IION KEY	NOLINA NOLINA	ddddddd	9999999	++++++++	0000000	hhhhhhhh			
			BUTION	BE USED							

1998/4/30

START 1998/4/1

ß

eeeeeee

fffffff

DISTRIBUTION Addddddd KEY TO BE USED

**AVAILABLE PERIOD** 

VERSION OF DISTRIBUTION KEY

DISTRIBUTION

DISTRIBUTION KEYS HELD BY RECEIVER

TRANSMIT DISTRIBUTION KEY 1998/5/1 1998/5/31 1998/6/1 1998/6/30

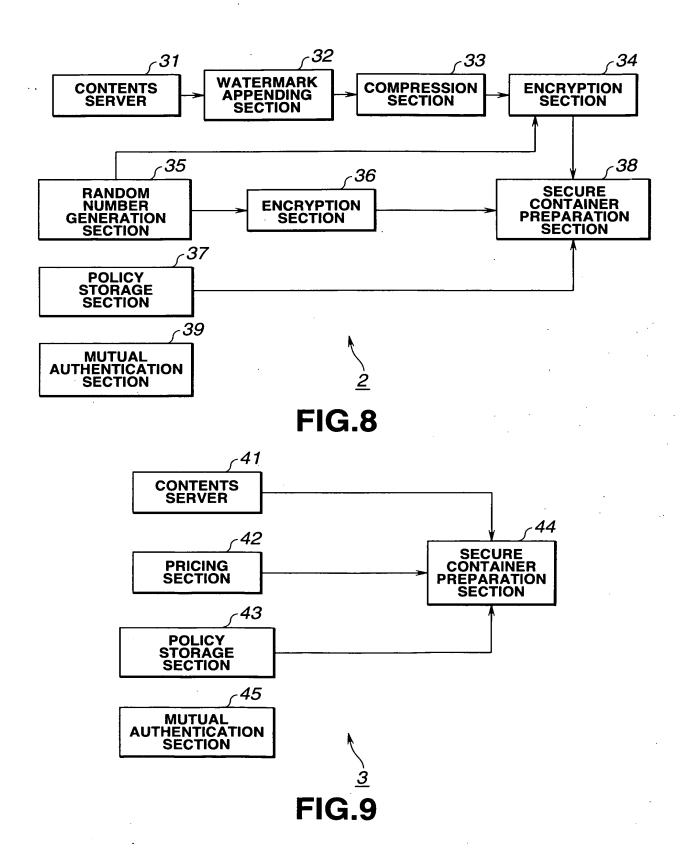
. .

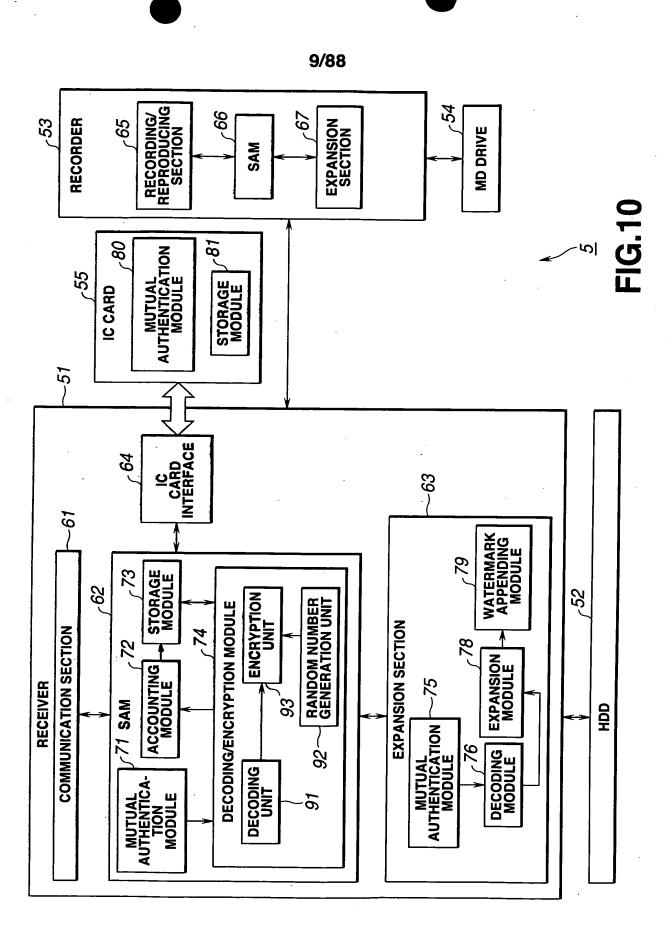
		· · · · · ·					<del></del>		<del></del> 1	1		<b>⁄88</b>
CE CENTER	AVAILABLE PERIOD	END	1998/1/31	1998/2/28	1998/3/31	1998/4/30	1998/5/31	1998/6/30	1998/7/31	1998/8/31	1998/9/30	
EMD SERVI	AVAILABL	START	1998/1/1	1998/2/1	1998/3/1	1998/4/1	1998/5/1	1998/6/1	1/2/8661	1998/8/1	1998/9/1	
EYS HELD BY	VERSION OF	KEY	-	2	က	4	5	9	7	∞	6	
DISTRIBUTION KEYS HELD BY EMD SERVICE CENTER	DISTRIBUTION		aaaaaaa	qqqqqqqq	2222222	ppppppppp	eeeeeee	ffffffff	99999999	hhhhhhhh		
			DISTRIBUTION KFY TO BE USED			_	TOANCHIT	DISTRIBUTION	KEY	7		
CONTENTS PROVIDER	AVAILABLE PERIOD	END	1998/4/30	1998/5/31	1998/6/30	1998/7/31	998/8/1 1998/8/31	1998/9/30				
	l	START	1998/4/1	1998/5/1	1998/6/1	1/2/8661	1998/8/1	1998/9/1				
KEYS HELD E	VERSION OF	DISTRIBUTION	4	5	9	7	8	6				
DISTRIBUTION KEYS HELD BY	NOTEIBILION	KEY	pppppppp	eeeeeee	fffffff	99999999	hhhhhhhh					
u			NO SE									

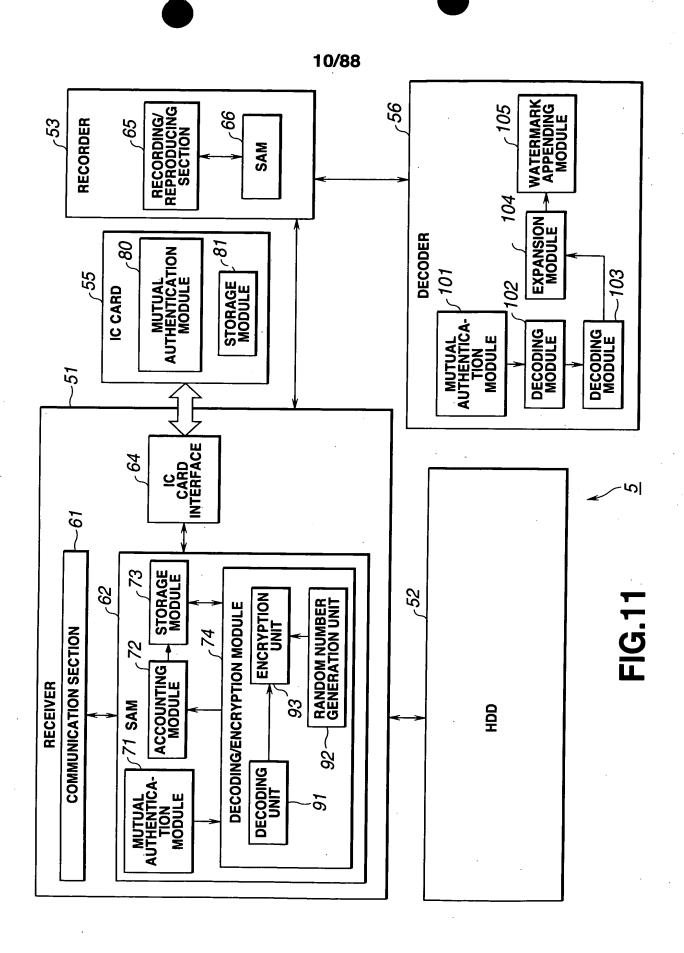
9.5

ID	SETTLEMENT PROCESSING	REGISTRATION	CONNECTION WITH EMD SERVICE CENTER
000000000000001h	POSSIBLE	POSSIBLE	POSSIBLE
0000000000000002h	POSSIBLE	POSSIBLE	IMPOSSIBLE
000000000000003h	POSSIBLE	IMPOSSIBLE	POSSIBLE
0000000000000004h	POSSIBLE	IMPOSSIBLE	IMPOSSIBLE
000000000000005h	IMPOSSIBLE	POSSIBLE	POSSIBLE
0000000000000006h	IMPOSSIBLE	POSSIBLE	IMPOSSIBLE
000000000000007h	IMPOSSIBLE	IMPOSSIBLE	POSSIBLE
000000000000008h	IMPOSSIBLE	IMPOSSIBLE	IMPOSSIBLE
0000000000000009h	POSSIBLE	POSSIBLE	POSSIBLE
• • •			
FFFFFFFFFFFEh	POSSIBLE	IMPOSSIBLE	IMPOSSIBLE
FFFFFFFFFFFFF	IMPOSSIBLE	POSSIBLE	POSSIBLE

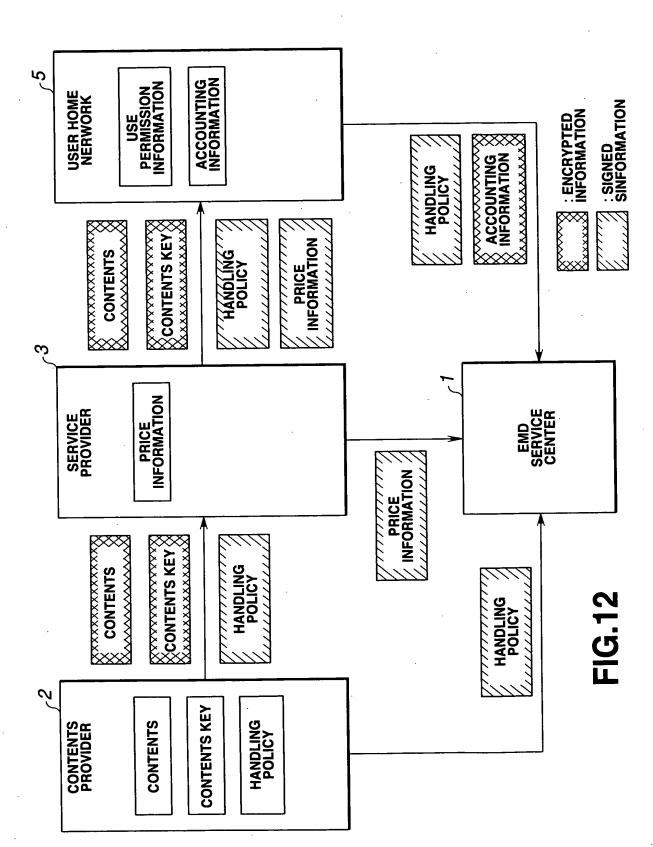
FIG.7







11/88



CONTENTS PROVIDER SECURE CONTAINER
CONTENTS KEY Kco
CONTENTS
DISTRIBUTION KEY Kd
CONTENTS KEY Kco
HANDLING POLICY
SECRET KEY OF CONTENTS PROVIDER Kscp
SIGNATURE
HASH FUNCTION
CONTENTS KEY Kco
CONTENTS
DISTRIBUTION KEY Kd
CONTENTS KEY Kco
HANDLING POLICY

**FIG.13** 

	ON NUMBER OF CERTIFICATE
SER ALLOCAT	IAL NUMBER OF CERTIFICATE FED BY AUTHENTICATION STATION
.GORITHM	AND PARAMETER USED FOR SIGNATURE
NAME	OF AUTHENTICATION STATION
EXPIR	ATION DATE OF CERTIFICATE
NAME	OF CONTENTS PROVIDER (ID)
JBLIC KE	EY OF CONTENTS PROVIDER Kpc
ECRET KE	EY OF AUTHENTICATION STATION Ksca
	SIGNATURE
A	HASH FUNCTION
VERS	SION NUMBER OF CERTIFICATE
	SERIAL NUMBER OF ERTIFICATE ALLOCATED BY AUTHENTICATION STATION
	GORITHM AND PARAMETER USED FOR SIGNATURE
	OF AUTHENTICATION STATION
NAME	//
NAME EXPI	RATION DATE OF CERTIFICATE
NAME EXPI	
NAME EXPI NAM	RATION DATE OF CERTIFICATE  ME OF CONTENTS PROVIDER

**FIG.14** 

	SERVICE PROVIDER
	SECURE CONTAINER
	CONTENTS KEY Kco
	CONTENTS
	DISTRIBUTION KEY Kd
	CONTENTS KEY Kco
	HANDLING POLICY
	PRICE INFORMATION
SECI	RET KEY OF SERVICE PROVIDER Kssp
	SIGNATURE
	HASH FUNCTION
	A CONTENTS MEY MAS
	CONTENTS KEY Kco CONTENTS
	DISTRIBUTION KEY Kd
	CONTENTS KEY Kco
	HANDLING POLICY
	PRICE INFORMATION

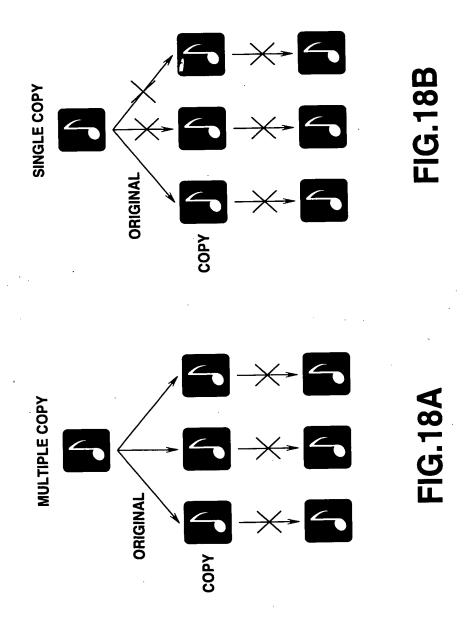
**FIG.15** 

(	CERTIFICATE OF SERVICE PROVIDER
	VERSION NUMBER OF CERTIFICATE
AL	SERIAL NUMBER OF CERTIFICATE LOCATED BY AUTHENTICATION STATION
ALGO	DRITHM AND PARAMETER USED FOR SIGNATURE
1	NAME OF AUTHENTICATION STATION
	EXPIRATION DATE OF CERTIFICATE
	NAME OF SERVICE PROVIDER (ID)
PU	BLIC KEY OF SERVICE PROVIDER Kpsp
SEC	CRET KEY OF AUTHENTICATION STATION Ksca
	SIGNATURE
	HASH FUNCTION
	VERSION NUMBER OF CERTIFICATE
	SERIAL NUMBER OF CERTIFICATE ALLOCATED BY AUTHENTICATION STATION
	ALGORITHM AND PARAMETER USED FOR SIGNATURE
	NAME OF AUTHENTICATION STATION
	EXPIRATION DATE OF CERTIFICATE
	NAME OF SERVICE PROVIDER (ID)
	PUBLIC KEY OF SERVICE PROVIDER Kpsp
V/	

**FIG.16** 

FIG.17A HANDLING AVAILABILITY	USE	PLAYBACK	Van E COBV	
POLICY			SINGLE COL 1	MULTIPLE COPY
	ILABILITY	1	0	-
				,
	USE	PLAYBACK	SINGLE COPY	MULTIPLE COPY
FIG. 17B POLICY AND AVAILABILITY	ILABILITY	-	0	1
INFORMATION PRICE	PRICE	150YEN	1	80YEN
				·
asn OSE OSE OSE	USE	PLAYBACK	SINGLE COPY	MULTIPLE COPY
TIG. I C PERMISSION AVAILABILITY	VILABILITY	-	0	0

17/88



**30YEN** 

80YEN

**150YEN** 

DISTRIBUTION

60YEN

MULTIPLE COPY

SINGLE COPY

PLAYBACK

USE

USE	AVAILAB	1000
	HANDLING POLICY AND	DISTRIBUTION
	FIG 19A	

USE	PLAYBACK	SINGLE COPY	MULTIPLE COPY
AVAILABILITY	۲ 1	0	-
PROFIT DISTRIBUTION	N 70YEN	•	40YEN



HANDLING POLICY, PROFI DISTRIBUTION AND PRICE
$\mathbf{\omega}$
0
T

<b>AVAILABILITY</b>	PROFIT DISTRIBUTION
HANDLING POLICY PROCEIT	DISTRIBUTION AND PRICE INFORMATION

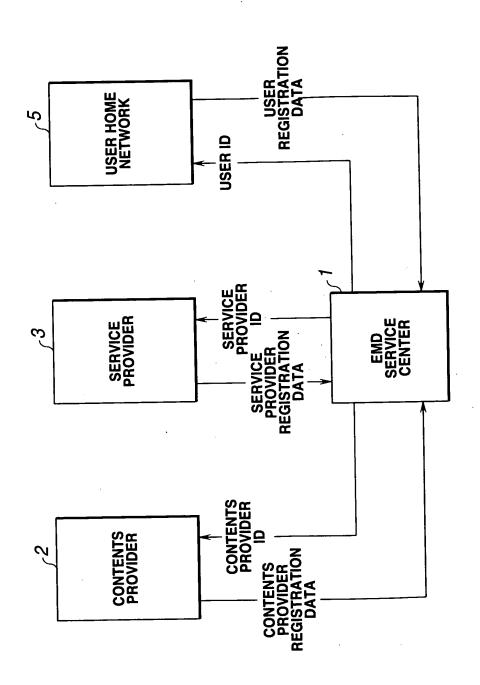


MULTIPLE COPY	0
SINGLE COPY	0
PLAYBACK	1
USE	NUMBER OF TIMES OF USE

FIG.19C ACCOUNTING INFORMATION

				PLAY BACK	
	ΞĞ	USE	UNLIMITED	LIMITED BY NUMBER OF TIMES	LIMITED BY DATE
FIG.ZUA	PRICE			5	1998/12/31
		PRICE	•	60 YEN	90 YEN
	J				
				PLAYBACK	
FIG. 20B	PER	USE	UNLIMITED	LIMITED BY NUMBER OF TIMES	LIMITED BY DATE
			,	5	•
		·			
,	<u>ב</u>			PLAYBACK	
FIG.20C PERMISSION INFORMATION	PERMISSION INFORMATION	USE	UNLIMITED	LIMITED BY NUMBER OF TIMES	LIMITED BY DATE
				2	

20/88

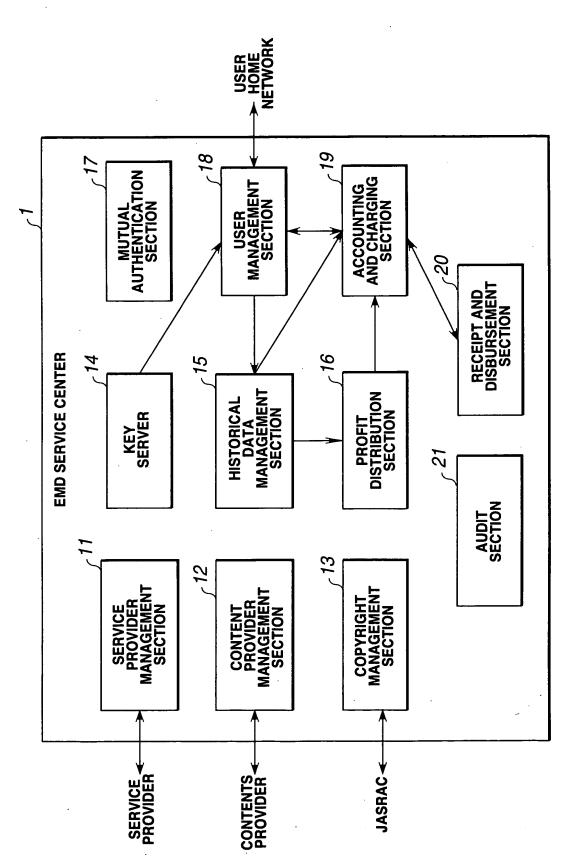


**FIG.2** 

CONTENTS ID	CONTENTS PROVIDER ID	ENTITLED ORGANIZATION
1	201	10%
2	201	20%

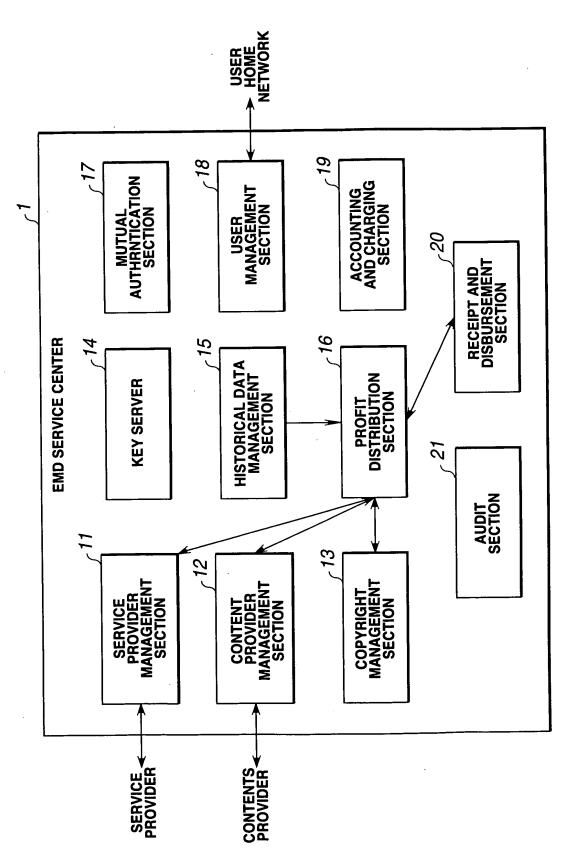
PROVIDER ID	CONTENTS ID	DISCOUNT	PERIOD
CONTENTS PROVIDER 1	•	7%	1998.9~1998.12
	2	3%	
	ALL CONTENTS	1%	
CONTENTS PROVIDER 2	3	%5	
SERVICE PROVIDER 1	1	3%	
SERVICE PROVIDER 2	4	1%	

MONTHLY FIXED RATE		VARIABLE RATE	
4000	PERIOD	1998.8~1998.9	-10%
1000YEN	FEE	3000YEN OR MORE	-5%



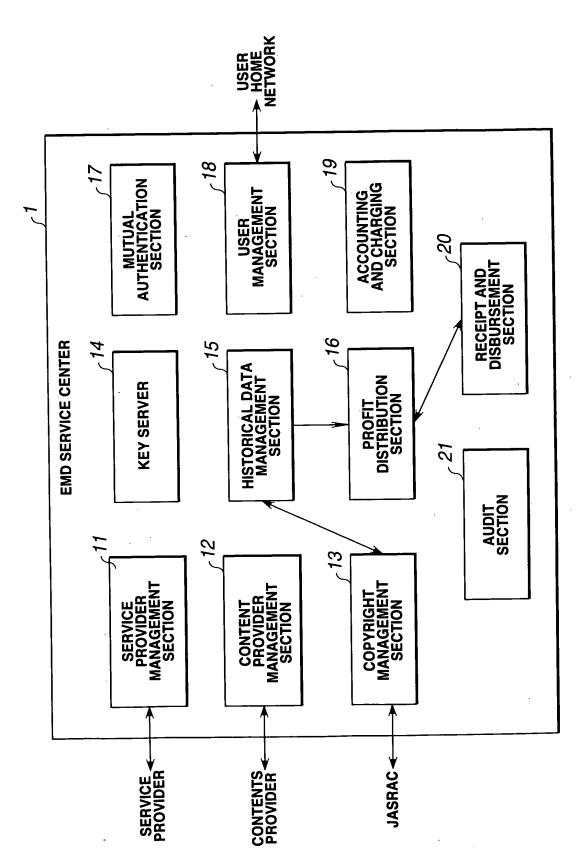
**FIG.25** 

25/88



**FIG.26** 

26/88



**FIG.27** 

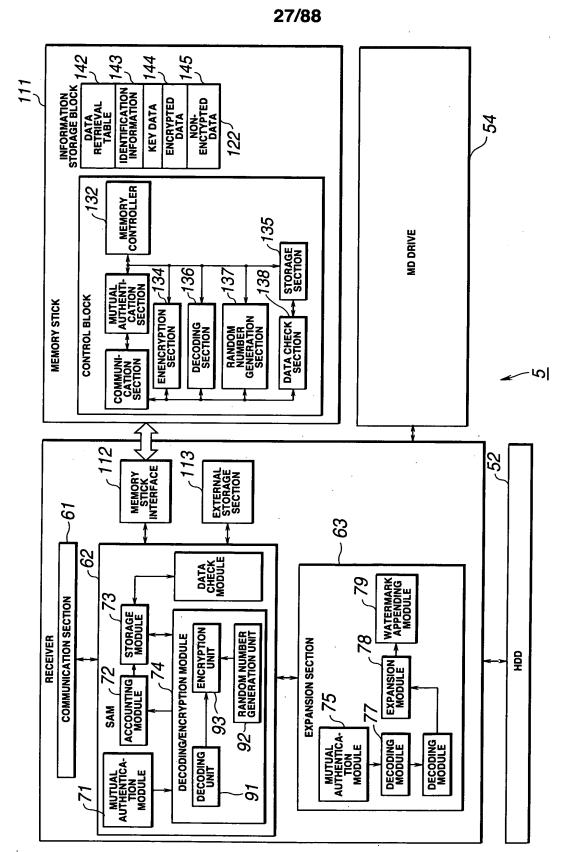


FIG.28

KEY DATA CONTENTS BLOCK 2 KEY 3	CONTENTS ID 3	USE PERMISSION INFORMATION 3	CONTENTS KEY 4	CONTENTS	
_				ID 4	USE PERMISSION INFORMATION 4
KEY DATA CONTENTS BLOCK 3 KEY 5	CONTENTS ID 5	USE PERMISSION INFORMATION 5			
KEY DATA BLOCK 4			CONTENTS KEY 6	CONTENTS ID 6	USE PERMISSION INFORMATION 6
KEY DATA BLOCK 5					

		SECRET KEY		
	ACCOL	UNTING INFORM	ATION	
		SAVE KEY		
	D	ISTRIBUTION KE	Υ	
		• • •		
CHECK VALUE 1	CHECK VALUE 2	CHECK VALUE 3	CHECK VALUE 4	CHECK VALUE 5

	CONTENTS KEY 1	CONTENTS ID 1	USE PERMISSION INFORMATION 1	CONTENTS KEY 2	CONTENTS ID 2	USE PERMISSION INFORMATION 2
	CONTENTS KEY 3	CONTENTS ID 3	USE PERMISSION INFORMATION 3	CONTENTS KEY 4	CONTENTS ID 4	USE PERMISSION INFORMATION 4
	CONTENTS KEY 5	CONTENTS ID 5	USE PERMISSION INFORMATION 5			
				CONTENTS KEY 6	CONTENTS ID 6	USE PERMISSION INFORMATION 6
<u> </u>						
	CHECK VALUE 1	CHECK VALUE 2	CHECK VALUE 3	CHECK VALUE 4	CHECK VALUE 5	
•						

	SECRET KEY	·
	ACCOUNTING INFORMATION	
·	SAVE KEY	
	DISTRIBUTION KEY	
	CHECK KEY	
	• • •	

KEY DATA BLOCK 1	CONTENTS KEY 1	CONTENTS ID 1	USE PERMISSION INFORMATION 1	CONTENTS KEY 2	CONTENTS ID 2	USE PERMISSION INFORMATION 2
KEY DATA BLOCK 2	CONTENTS KEY 3	CONTENTS ID 3	USE PERMISSION INFORMATION 3	CONTENTS KEY 4	CONTENTS ID 4	USE PERMISSION INFORMATION 4
KEY DATA BLOCK 3	CONTENTS KEY 5	CONTENTS ID 5	USE PERMISSION INFORMATION 5			
KEY DATA BLOCK 4	CONTENTS KEY 6	CONTENTS ID 6	USE PERMISSION INFORMATION 6			

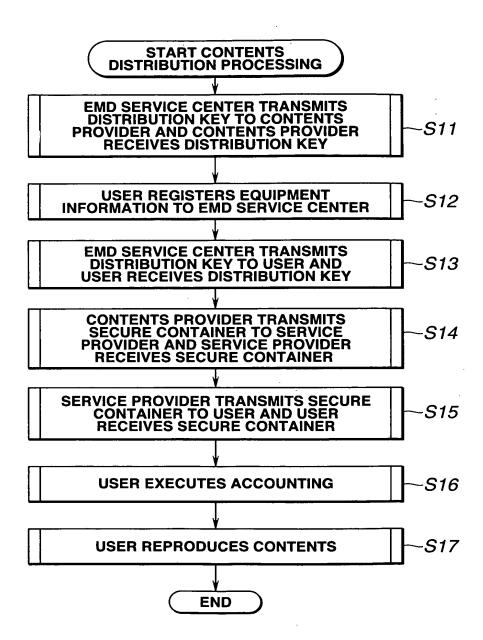
SECRET KEY					
	SAVE	KEY			
	_				
	•	• •			
CHECK VALUE 1	CHECK VALUE 2	CHECK VALUE 3	CHECK VALUE 4		

CHECK VALUE 4		CHECK VALUE 3	CHECK VALUE 2		CHECK VALUE 1
·			USE PERMISSION INFORMATION 6	CONTENTS ID 6	CONTENTS KEY 6
			USE PERMISSION INFORMATION 5	CONTENTS ID 5	CONTENTS KEY 5
USE PERMISSION INFORMATION 4	CONTENTS ID 4	CONTENTS KEY 4	USE PERMISSION INFORMATION 3	CONTENTS ID 3	CONTENTS KEY 3
USE PERMISSION INFORMATION 2	CONTENTS ID 2	CONTENTS KEY 2	USE PERMISSION INFORMATION 1	CONTENTS ID 1	CONTENTS KEY 1

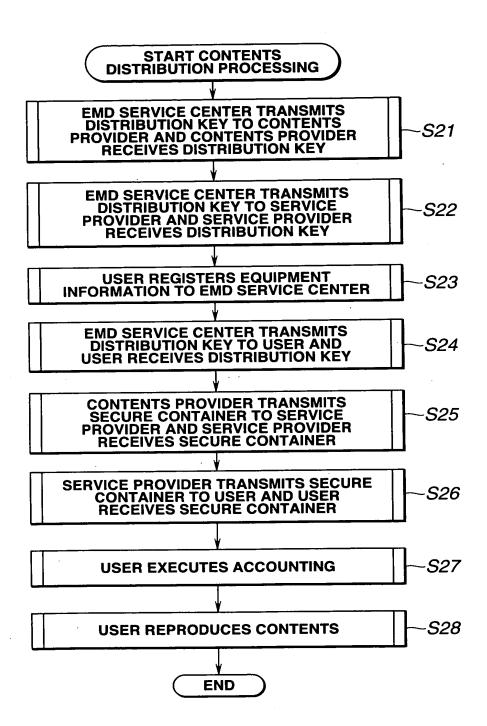
SECRET KEY	
CHECK KEY	
SAVE KEY	
• • •	
	•

**FIG.36** 

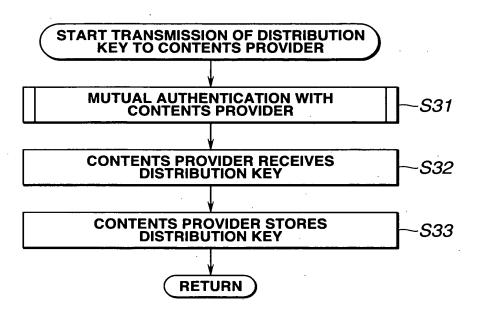
-



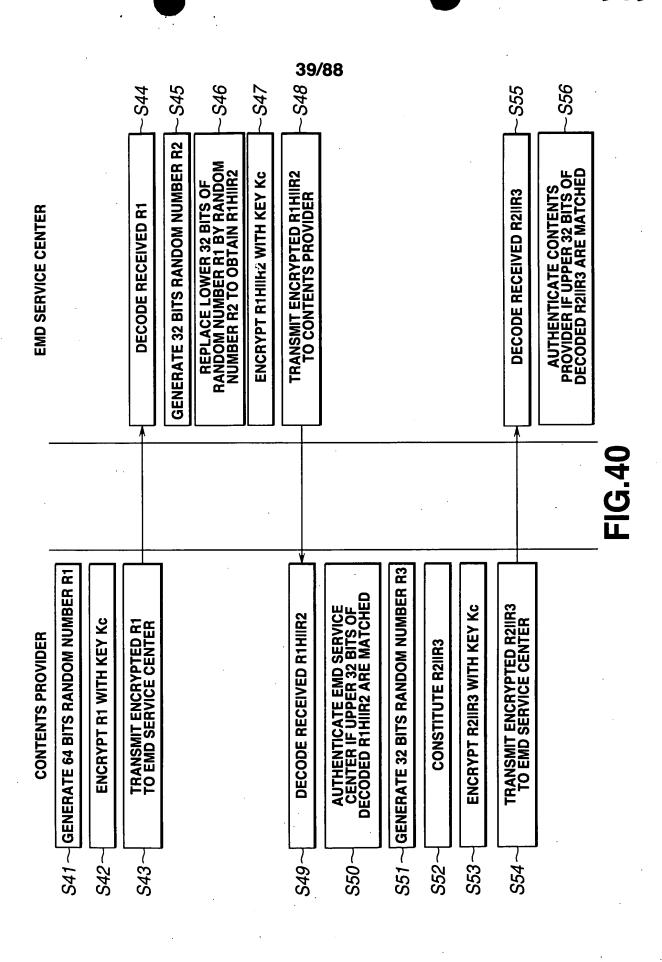
**FIG.37** 



**FIG.38** 



**FIG.39** 



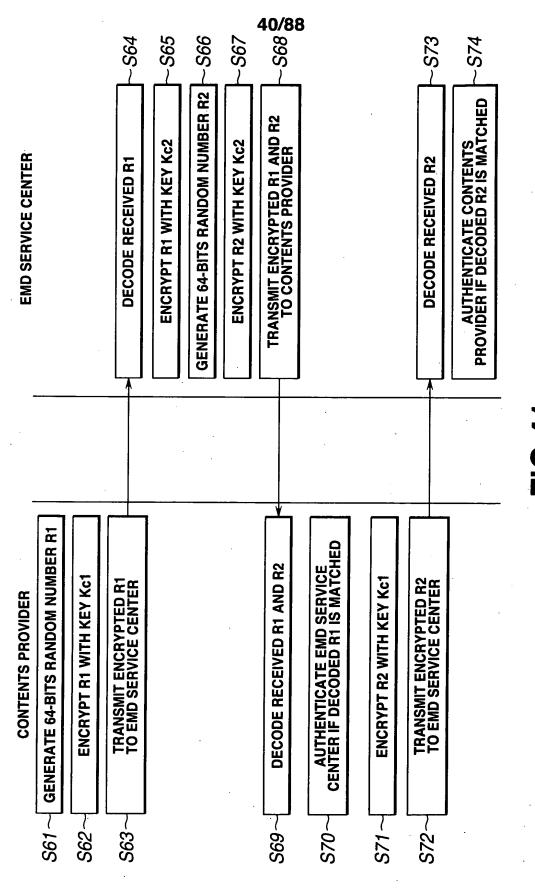
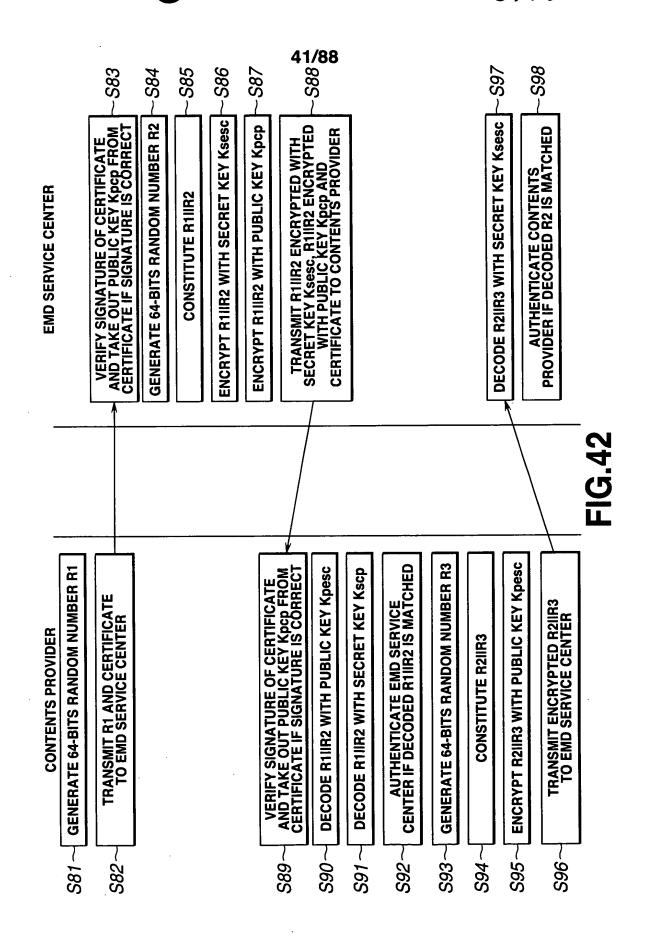
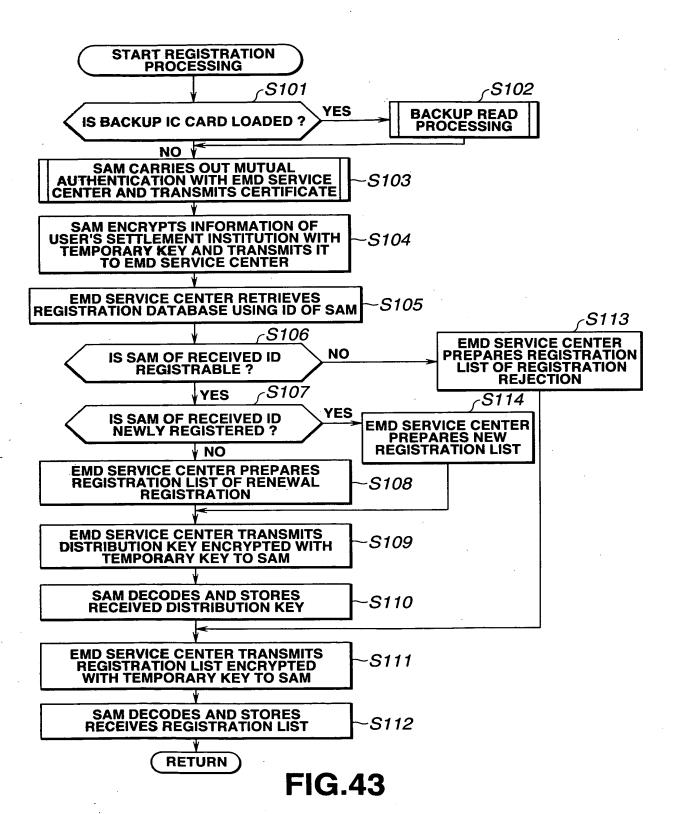


FIG.41





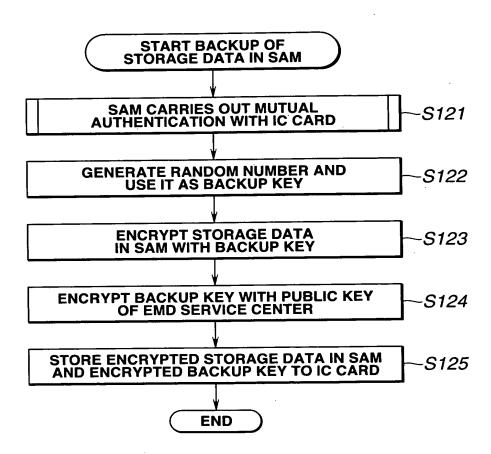


# **CERTIFICATE OF SAM VERSION NUMBER OF CERTIFICATE** SERIAL NUMBER OF CERTIFICATE ALLOCATED BY AUTHENTICATION STATION ALGORITHM AND PARAMETER USED FOR SIGNATURE NAME OF AUTHENTICATION STATION **EXPIRATION DATE OF CERTIFICATE** NAME OF SAM (ID) **PUBLIC KEY OF SAM Kpu** PARAMETER INDICATING WHETHER IT IS DEPENDENT UPON ANOTHER SAM **SECRET KEY OF AUTHENTICATION STATION Ksca SIGNATURE** HASH FUNCTION VERSION NUMBER OF CERTIFICATE SERIAL NUMBER OF CERTIFICATE ALLOCATED BY AUTHENTICATION STATION ALGORITHM AND PARAMETER **USED FOR SIGNATURE** NAME OF AUTHENTICATION STATION **EXPIRATION DATE OF CERTIFICATE** NAME OF SAM (ID) PUBLIC KEY OF SAM Kpu PARAMETER INDICATING WHETHER IT IS DEPENDENT UPON ANOTHER SAM

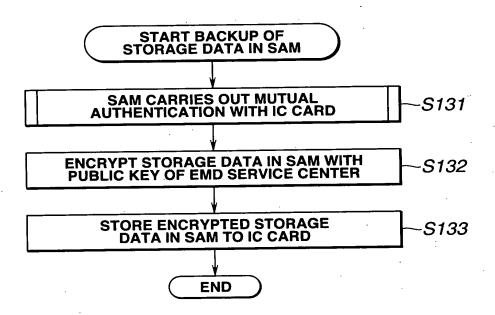
**FIG.44** 

<u> </u>				
SIGNATURE	XXXXXXXXX	XXXXXXXX	XXXXXXXX	XXXXXXXX
CONDITION FLAG (1 BIT)	0	1	1	1
STATUS FLAG (4 BITS)	0000	1010	1100	0000
REGISTRATION REJECTION FLAG (1 BIT)	1	1	1	0
ID OF SAM (64 BITS)	0000000000000001h	000000000000000000000	4E00000000000000000	000000000000000Ah

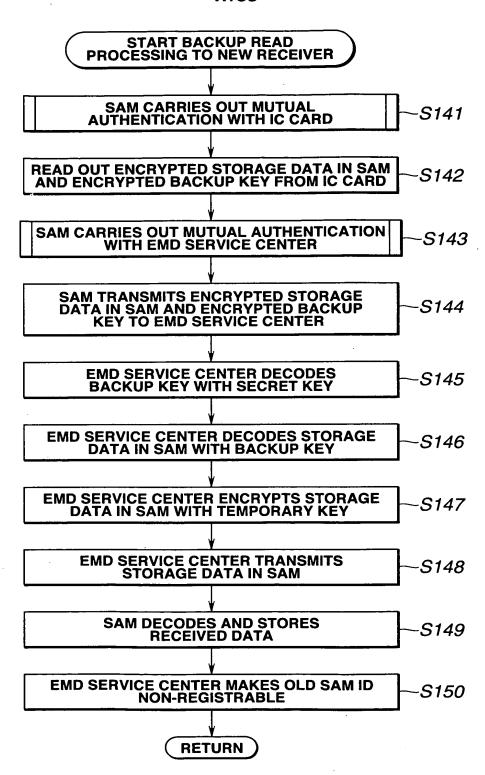
# **FIG.45**



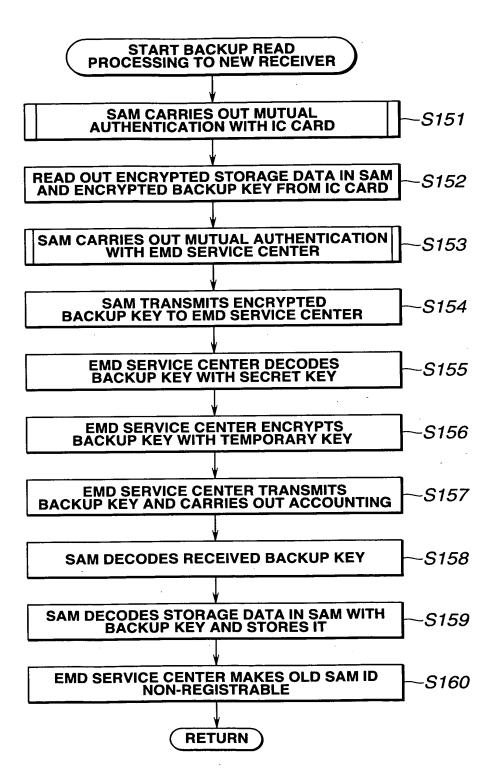
**FIG.46** 



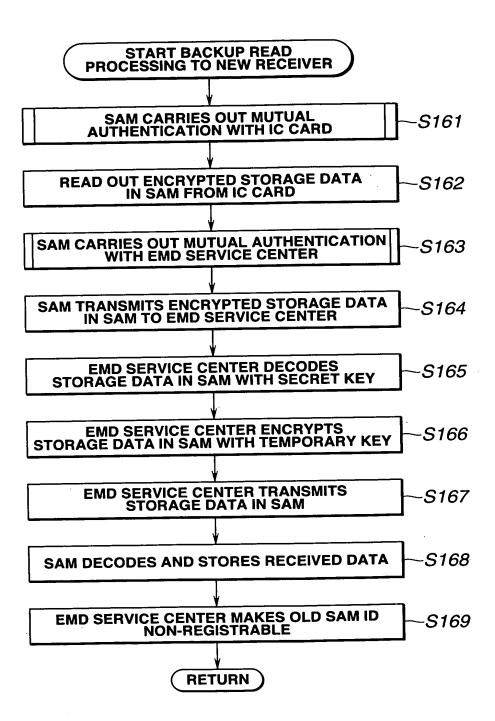
**FIG.47** 



**FIG.48** 



**FIG.49** 

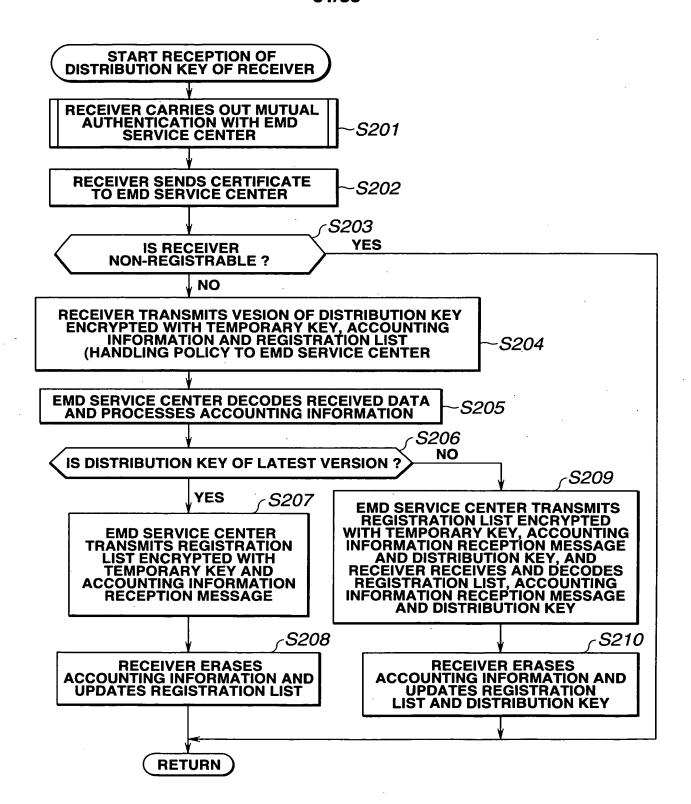


**FIG.50** 

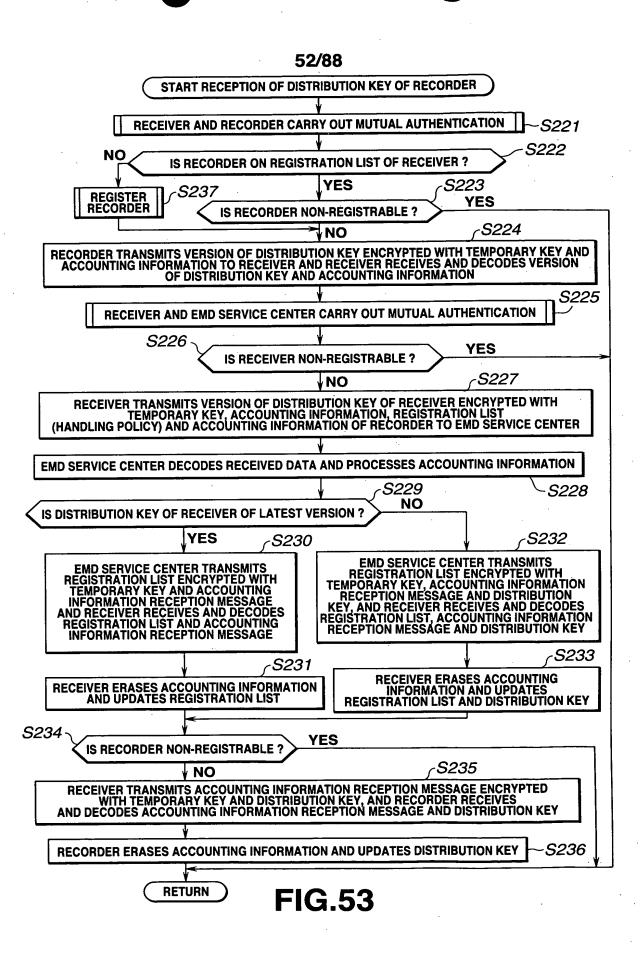
## 50/88 START RECORDER REGISTRATION PROCESSING RECEIVER ADDS RECORDER ID TO REGISTRATION LIST S181 RECEIVER AND EMD SERVICE CENTER CARRY OUT MUTUAL AUTHENTICATION S182 S183 YES IS RECEIVER NON-REGISTRABLE? **↓NO** RECEIVER TRANSMITS VERSION OF DISTRIBUTION KEY OF RECEIVER ENCRYPTED WITH TEMPORARY KEY, ACCOUNTING INFORMATION AND REGISTRATION LIST (HANDLING POLICY) TO EMD SERVICE CENTER ·S184 EMD SERVICE CENTER DECODES RECEIVED DATA, PROCESSES ACCOUNTING INFORMATION AND UPDATES REGISTRATION LIST ·S185 S186 IS DISTRIBUTION KEY OF RECEIVER OF LATEST VERSION? NO ·S189 YES EMD SERVICE CENTER TRANSMITS REGISTRATION LIST ENCRYPTED WITH TEMPORARY KEY, ACCOUNTING INFORMATION RECEPTION MESSAGE, AND RECEIVER RECEIVES, DECODES AND STORES REGISTRATION LIST, ACCOUNTING INFORMATION RECEPTION MESSAGE AND DISTRIBUTION KEY EMD SERVICE CENTER TRANSMITS REGISTRATION LIST ENCRYPTED WITH TEMPORARY KEY AND ACCOUNTING INFORMATION RECEPTION MESSAGE, AND RECEIVER RECEIVES, DECODES AND STORES REGISTRATION LIST AND ACCOUNTING INFORMATION RECEPTION MESSAGE ~S190 ~S188 RECEIVER ERASES ACCOUNTING INFORMATION AND UPDATES REGISTRATION LIST AND DISTRIBUTION KEY RECEIVER ERASES ACCOUNTING INFORMATION AND UPDATES REGISTRATION LIST S191 YES IS RECORDER NON-REGISTRABLE? RECEIVER AND RECORDER CARRY S192 OUT MUTUAL AUTHENTICATION -S193 RECEIVER TRANSMITS REGISTRATION COMPLETION MESSAGE ENCRYPTED WITH TEMPORARYO KEY AND DISTRIBUTION KEY, AND RECORDER RECEIVES AND DECODES REGISTRATION COMPLETION MESSAGE AND DISTRIBUTION KEY RECORDER UPDATES DISTRIBUTION KEY S194

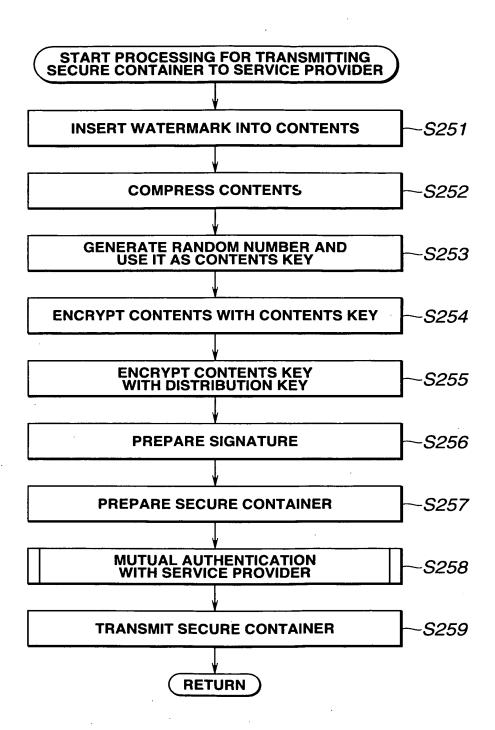
**FIG.51** 

RETURN

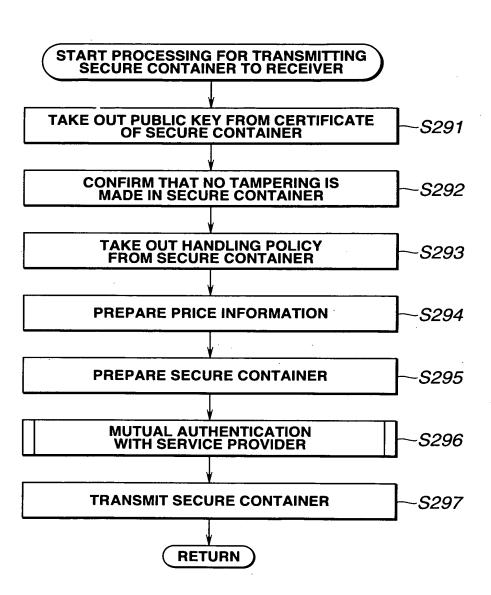


**FIG.52** 

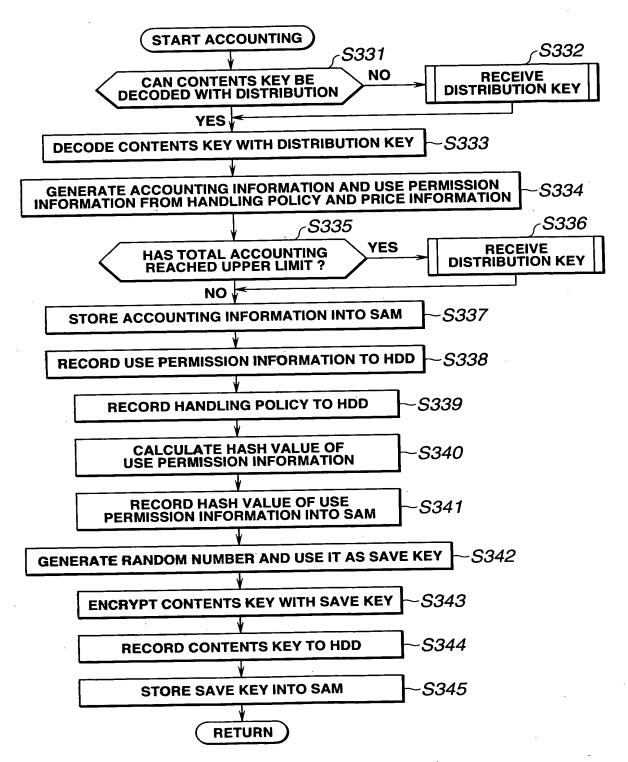




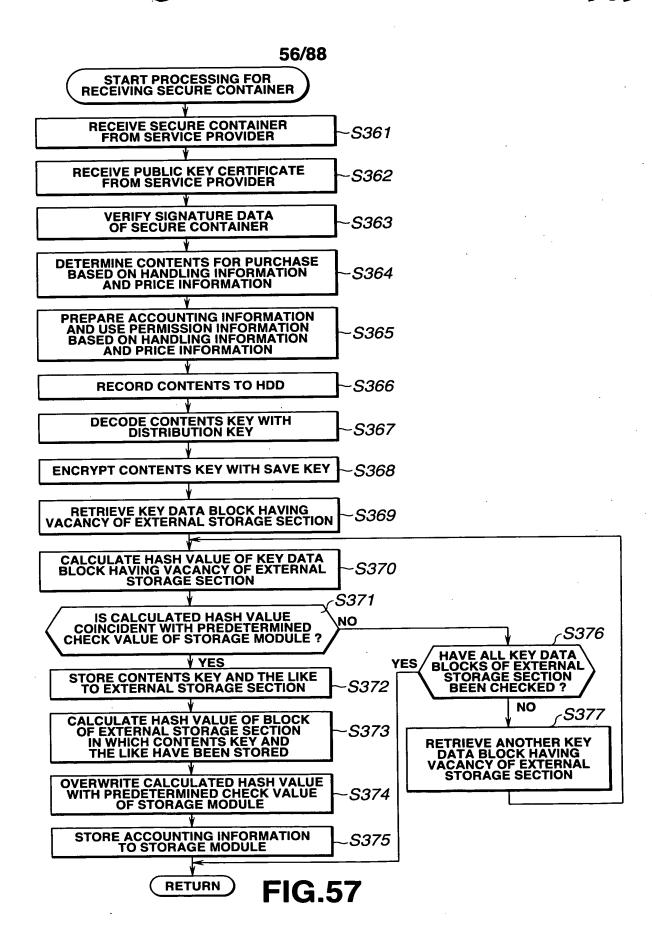
**FIG.54** 

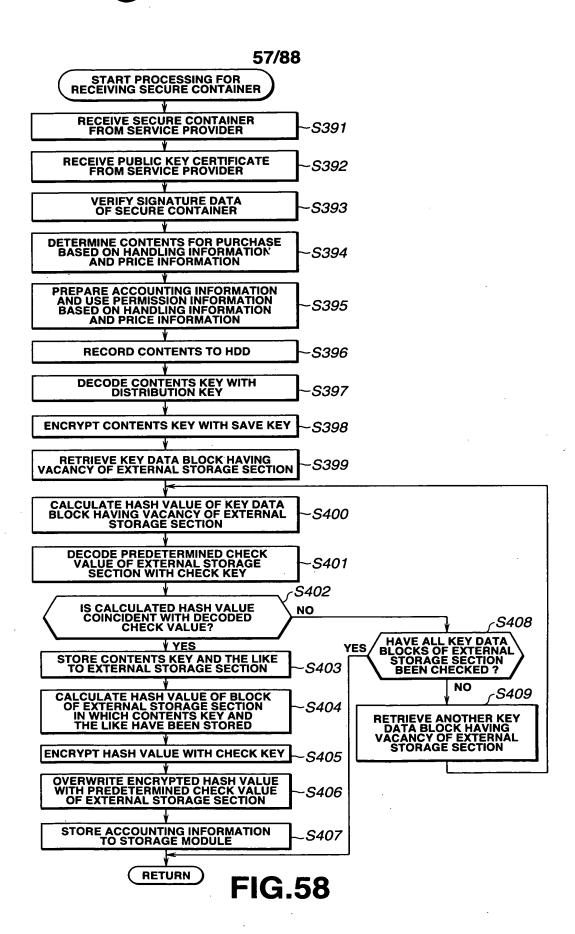


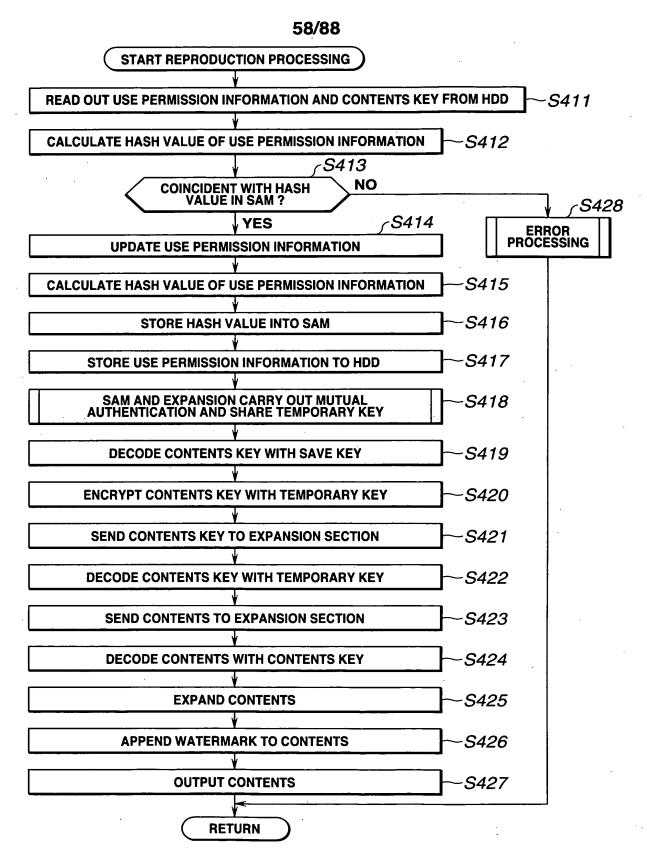
**FIG.55** 



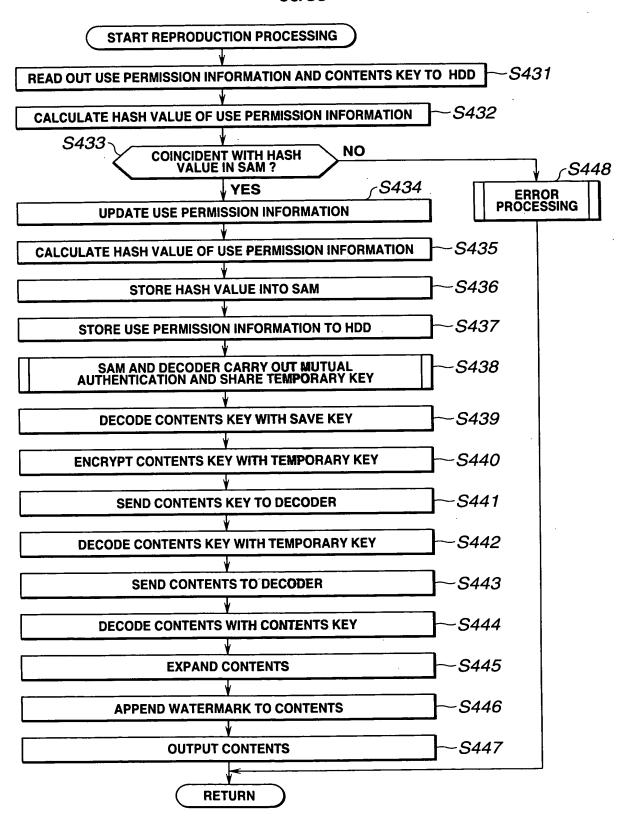
**FIG.56** 



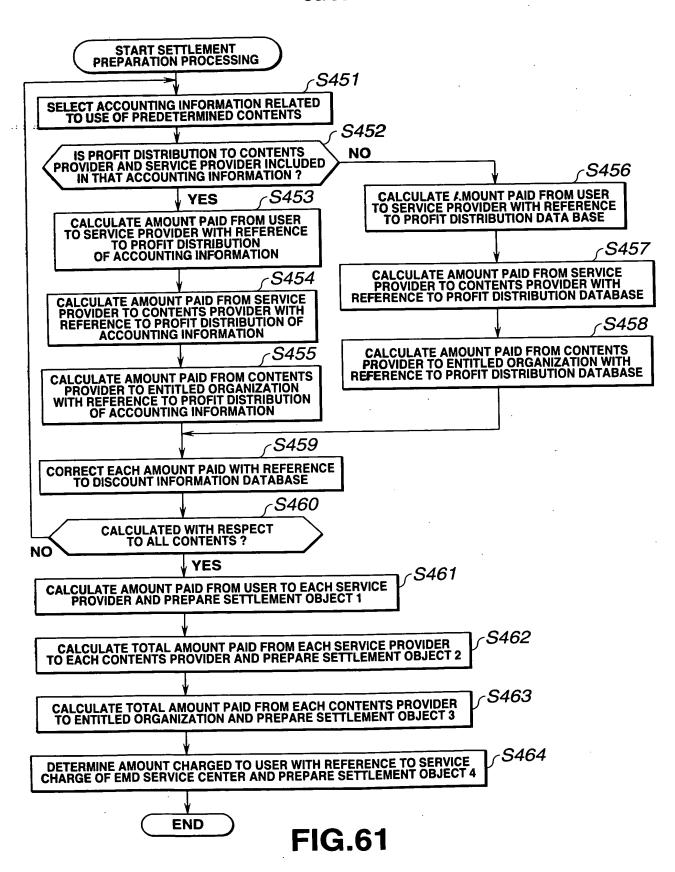




**FIG.59** 



**FIG.60** 



#### **CREDIT SETTLEMENT OBJECT 1**

FIG.62A

PAYER : USER ID

AMOUNT CHARGED : X PAYEE : SERVICE PROVIDER ID AMOUNT PAID : x1

#### **CREDIT SETTLEMENT OBJECT 2**

FIG.62B

PAYER: CREDIT SETTLEMENT OBJECT 1

AMOUNT CHARGED : -PAYEE : CONTENTS PROVIDER ID AMOUNT PAID : x2

#### **CREDIT SETTLEMENT OBJECT 3**

**FIG.62C** 

PAYER : CREDIT SETTLEMENT OBJECT 1
AMOUNT CHARGED : -

PAYEE : ENTITLED ORGANIZATION ID AMOUNT PAID : x3

#### **CREDIT SETTLEMENT OBJECT 4**

FIG.62D

**PAYER: CREDIT SETTLEMENT OBJECT 1** 

AMOUNT CHARGED : -

PAYEE : EMD SERVICE CENTER ID AMOUNT PAID : x4

#### **BANK SETTLEMENT OBJECT 1**

FIG.63A

**PAYER: SERVICE PROVIDER ID** 

AMOUNT CHARGED : y1
PAYEE : EMD SERVICE CENTER ID

**AMOUNT PAID: y1** 

# BANK SETTLEMENT OBJECT 2

FIG.63B

**PAYER: CONTENTS PROVIDER ID** 

AMOUNT CHARGED : y2 PAYEE : EMD SERVICE CENTER ID

**AMOUNT PAID: y2** 

# BANK SETTLEMENT OBJECT 3

FIG.63C

**PAYER: ENTITLED ORGANIZATION ID** 

**AMOUNT CHARGED: y3** 

**PAYEE: EMD SERVICÉ CENTER ID** 

**AMOUNT PAID: y3** 

## CREDIT SETTLEMENT OBJECT 1

FIG.64A

PAYER : USER ID

**AMOUNT CHARGED: x** 

**PAYEE: SERVICE PROVIDER ID** 

**AMOUNT PAID: x1** 

# BANK SETTLEMENT OBJECT 2

FIG.64B

PAYER : SERVICE PROVIDER ID AMOUNT CHARGED : x2+x3

**PAYEE: CONTENTS PROVIDER ID** 

**AMOUNT PAID: x2+x3** 

#### BANK SETTLEMENT OBJECT 3

FIG.64C

**PAYER: CONTENTS PROVIDER ID** 

**AMOUNT CHARGED: x3** 

**PAYEE: ENTITLED ORGANIZATION ID** 

**AMOUNT PAID: x3** 

# CREDIT SETTLEMENT OBJECT 4

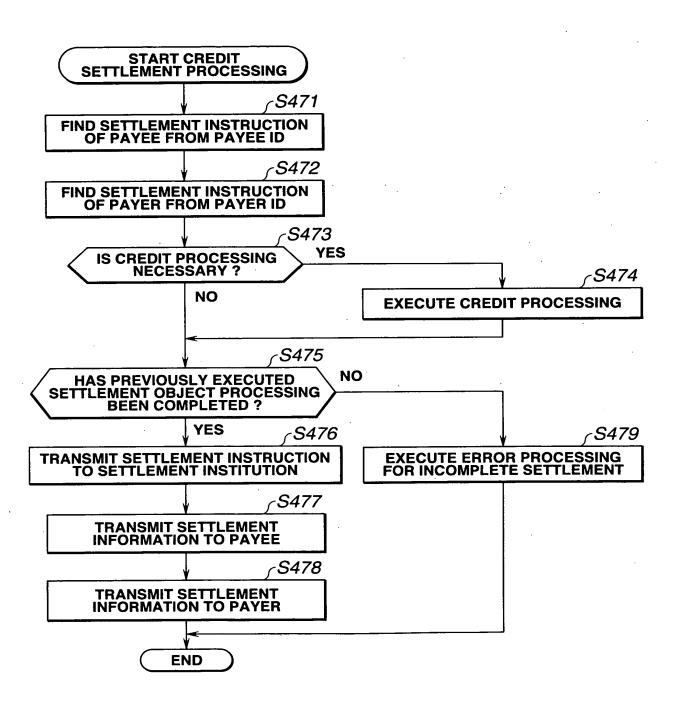
FIG.64D

**PAYER: CREDIT SETTLEMENT OBJECT 1** 

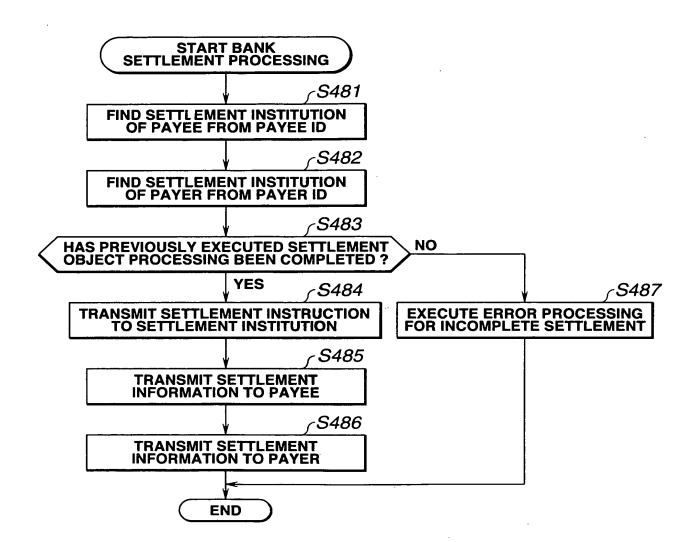
**AMOUNT CHARGED: -**

**PAYEE: EMD SERVICE CENTER ID** 

**AMOUNT PAID: x4** 

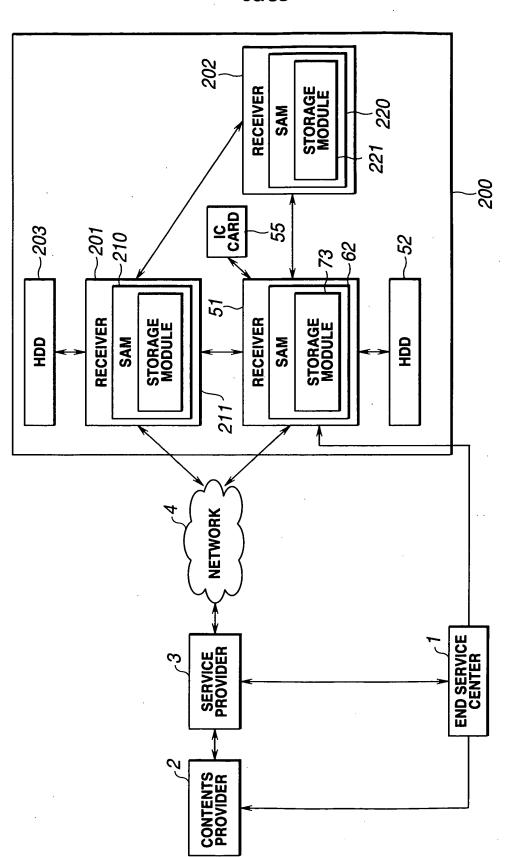


**FIG.65** 



**FIG.66** 

66/88



**FIG.67** 

PART						
REGISTRATION LIST SIGNATURE	× × ×					
REGISTRATION CONDITION SIGNATURE	×××	×××	× ×			
STATUS INFORMATION	UNLIMITED	UNLIMITED	UNLIMITED			
CONTENTS SUPPLY EQUIPMENT	NONE	NONE	ID OF SAM 62 ID OF	<b>SAM</b> 210		
ACCOUNTING EQUIPMENT	ID OF SAM 62	ID OF SAM 62	NONE			
ACCOUNTING	ALABLE AVAILABLE	UN- ALABLE AVAILABLE	UN- AILABLE AVAILABLE	-		
PURCHASE PROCESSING	AVAILABLE	AVAILABLE	UN- AVAILABLE			
USER	ID OF USER	ID OF USER	ID OF USER			
SAMID	ID OF SAM 62	ID OF SAM 210	ID OF SAM 220			
	CONDITION OF RECEIVER 51	REGISTRATION CONDITION OF RECEIVER 201	REGISTRATION CONDITION OF RECEIVER 202			

ID OF SAM 62 ×××× ××× က NUMBER OF EQUIPMENTS CONNECTED **EXPIRATION DATE VERSION NUMBER TARGET SAM ID** 

PART						
REGISTRATION REGISTRATION CONDITION LIST SIGNATURE SIGNATURE	×××					
REGISTRATION CONDITION SIGNATURE	×××	×××	×			
STATUS INFORMATION	UNLIMITED	UNLIMITED	UNLIMITED			
CONTENTS SUPPLY EQUIPMENT	NONE	NONE	ID OF SAM 62 ID OF	SAM 210		
ACCOUNTING EQUIPMENT	ID OF SAM 62	ID OF SAM 62	NONE		_	
ACCOUNTING	LABLE AVAILABLE	UN- LABLE AVAILABLE	IN- LABLE AVAILABLE			
PURCHASE PROCESSING	AVAILABLE	AVAILABLE	UN- AVAILABLE			
USER ID	ID OF USER	ID OF USER	ID OF USER			
SAM ID	ID OF SAM 62	ID OF SAM 210	ID OF SAM 220			
REGISTRATION CONDITION OF REGISTRATION CONDITION OF REGISTRATION CONDITION OF RECEIVER 201 RECEIVER 202 RECEIVER 202						

EXPIRATION DATE

EXPIRATION DATE

XXXX

IARGET SAM 210

ID OF SAM 210

IARGET SAM 210

INFORMA

PART

NUMBER OF EQUIPMENTS

3

**FIG.69** 

PART							
REGISTRATION REGISTRATION CONDITION LIST SIGNATURE SIGNATURE	×××					-	
	×××						
STATUS INFORMATION	UNLIMITED						
CONTENTS SUPPLY EQUIPMENT	ID OF SAM 62	ID OF SAM 210					
ACCOUNTING ACCOUNTING EQUIPMENT	NONE			٠.			
	UN- ILABLE AVAILABLE						
PURCHASE PROCESSING	UN- AVAILABLE						
USER ID	ID OF USER						
SAM ID	F ID OF SAM 220						

TARGET SAM ID

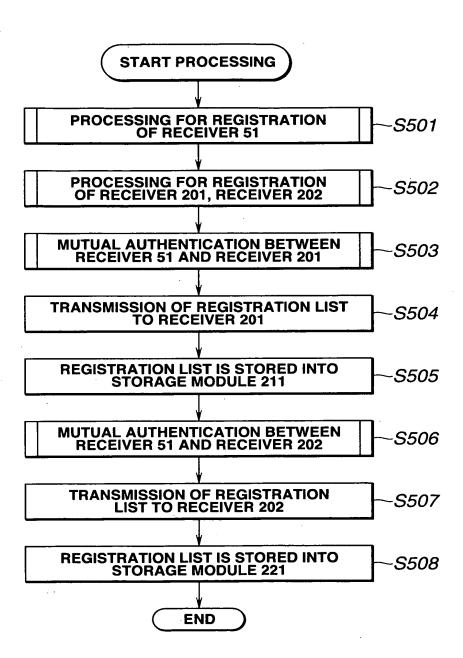
EXPIRATION DATE

XXXX

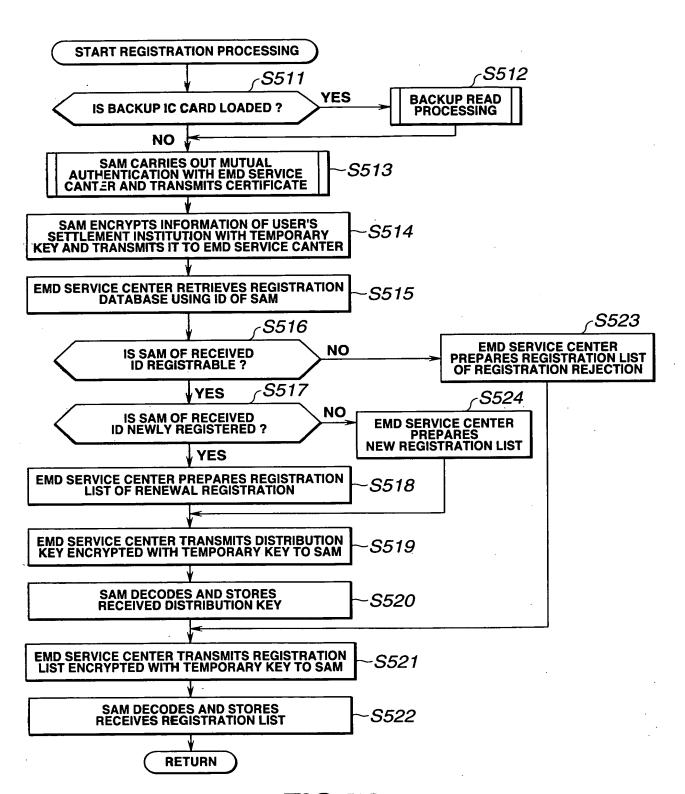
TARGET SAM 220

TARGET S

FIG.70



**FIG.71** 



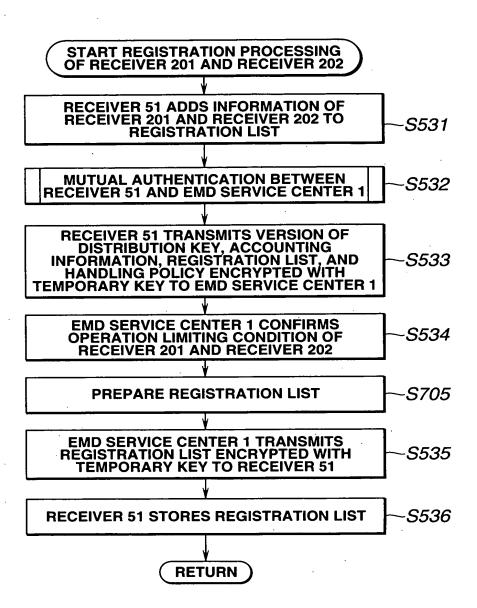
**FIG.72** 

		PART
REGISTRATION REGISTRATION CONDITION SIGNATURE SIGNATURE	× × ×	
	× ×	
STATUS INFORMATION	UNLIMITED	
CONTENTS SUPPLY EQUIPMENT	NONE	
ACCOUNTING EQUIPMENT	ID OF SAM 62	
ACCOUNTING	ILABLE AVAILABLE	·
PURCHASE PROCESSING	AVAILABLE	
USER	ID OF USER	
SAM ID	ID OF ID OF	

TARGET SAM VINFORMATION PART					
ID OF SAM 62	××××	××××	ဇ		
TARGET SAM ID	<b>EXPIRATION DATE</b>	VERSION NUMBER	NUMBER OF EQUIPMENTS CONNECTED		

**FIG.73** 

REGISTRATION LIST



**FIG.74** 

		_	PART		·	 	_
REGISTRATION LIST SIGNATURE	×××						,
REGISTRATION CONDITION SIGNATURE	× × ×	×	×××			 •.	
STATUS INFORMATION	UNLIMITED	UNLIMITED	UNLIMITED	ID OF SAM 210			
CONTENTS SUPPLY EQUIPMENT	NONE	NONE	ID OF SAM 62				
ACCOUNTING CONTENTS SUPPLY EQUIPMENT	ID OF SAM 62	ID OF SAM 62	NONE				
ACCOUNTING	ILABLE AVAILABLE	UN- ILABLE AVAILABLE	UN- ILABLE AVAILABLE				•
PURCHASE PROCESSING	AVAILABLE	AVAILABLE	UN- AVAILABLE				
USER	ID OF USER						
SAM ID	ID OF SAM 62	ID OF SAM 210	ID OF SAM 220				

EXPIRATION DATE

VERSION NUMBER OF EQUIPMENTS

TARGET S

INFORMAT

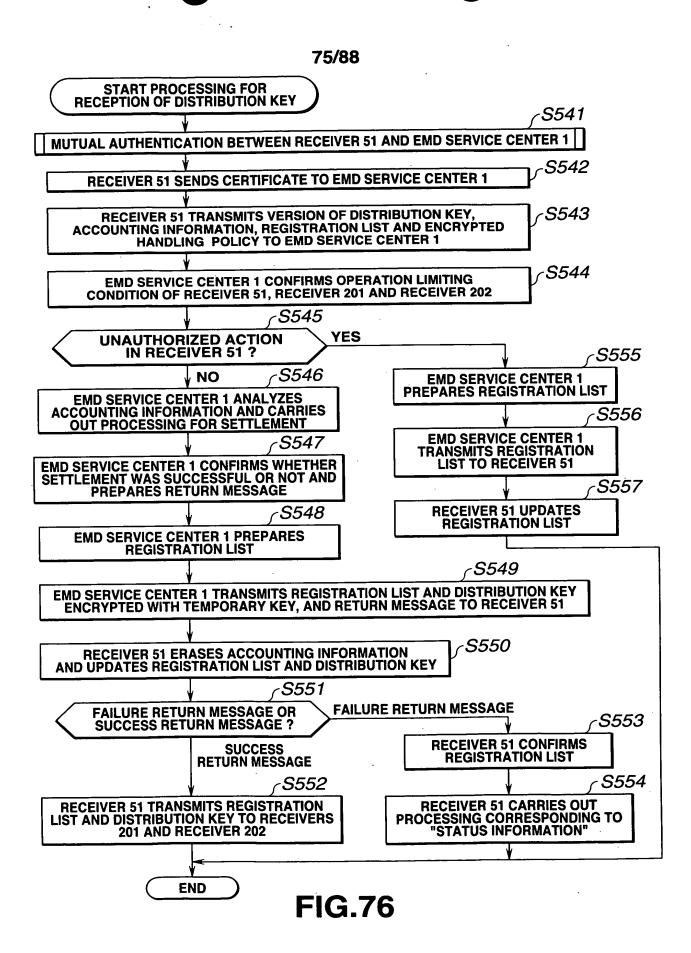
PART

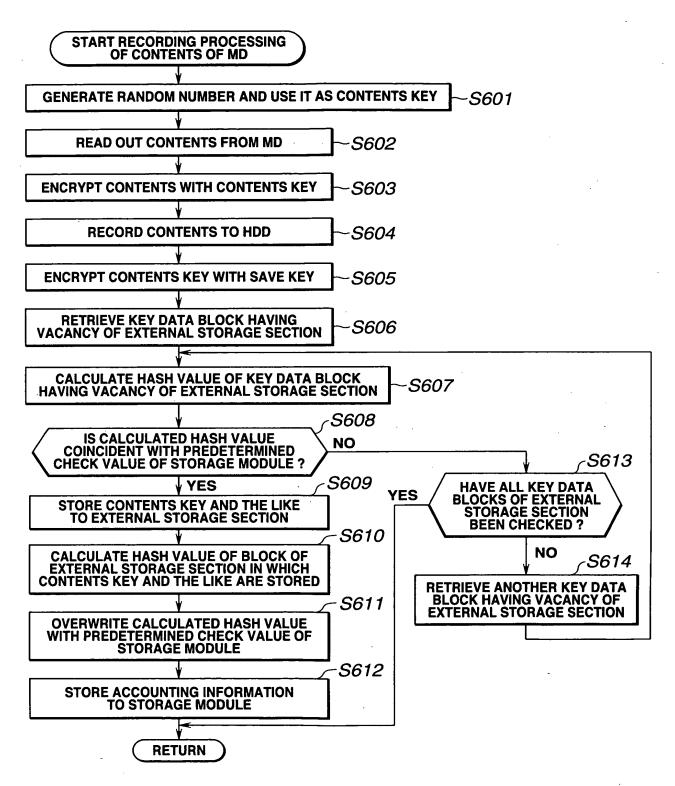
S

ONUMBER OF EQUIPMENTS

3

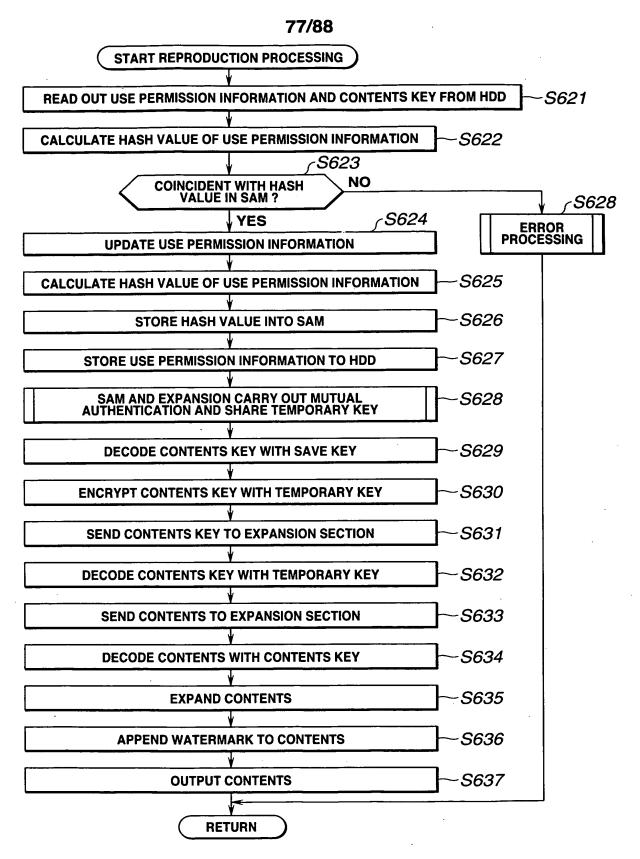
FIG.75



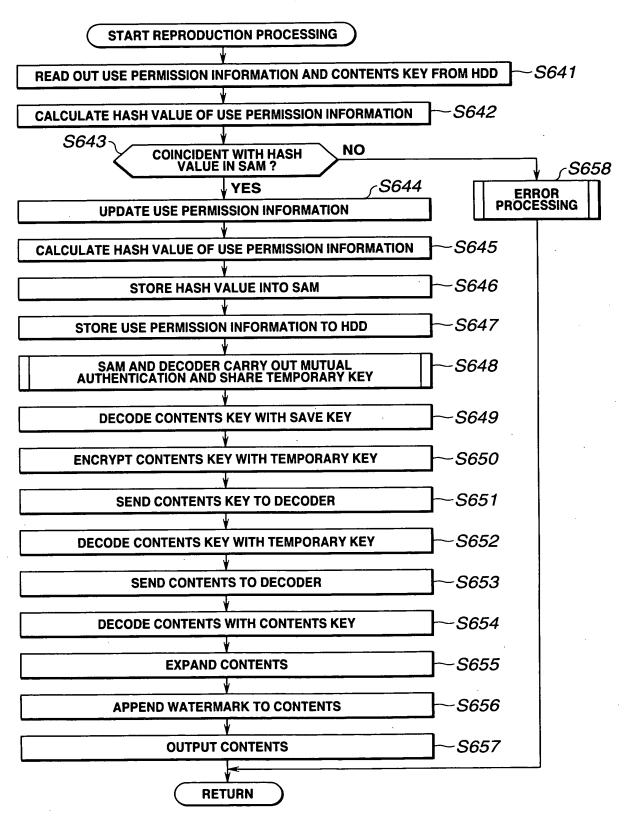


**FIG.77** 

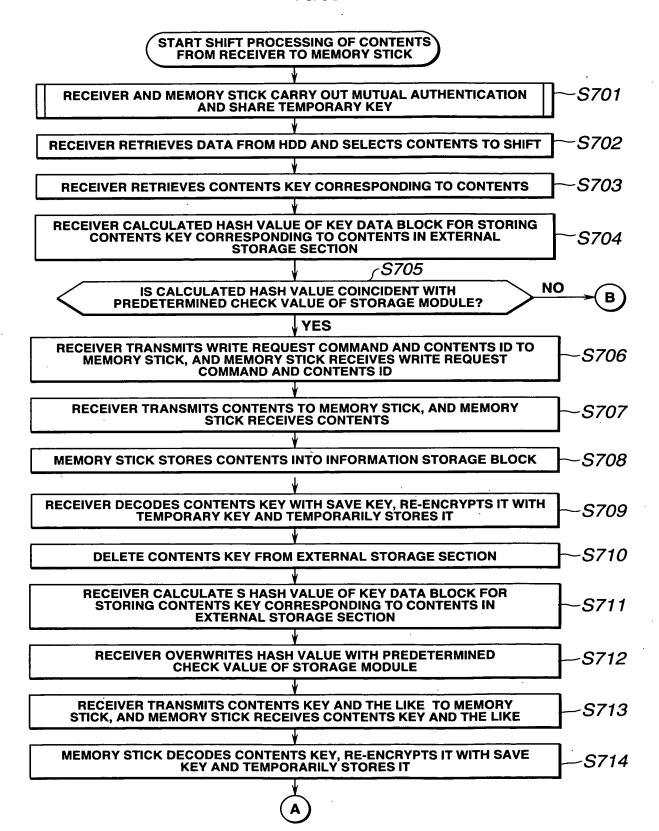
, it is a



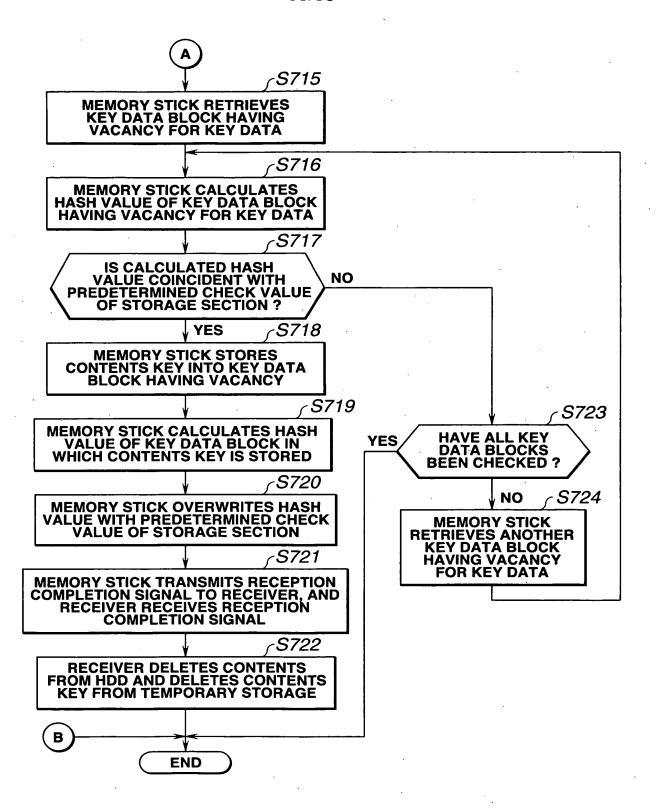
**FIG.78** 



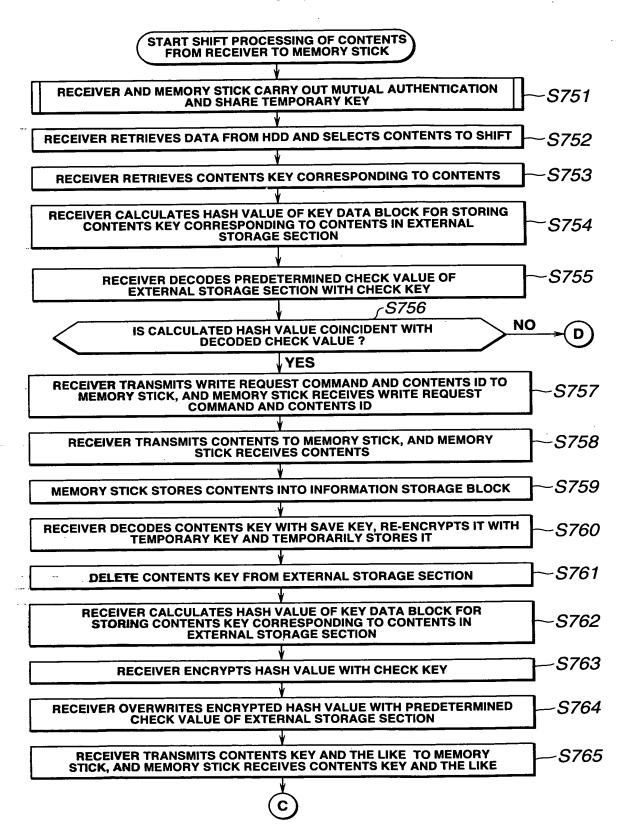
**FIG.79** 



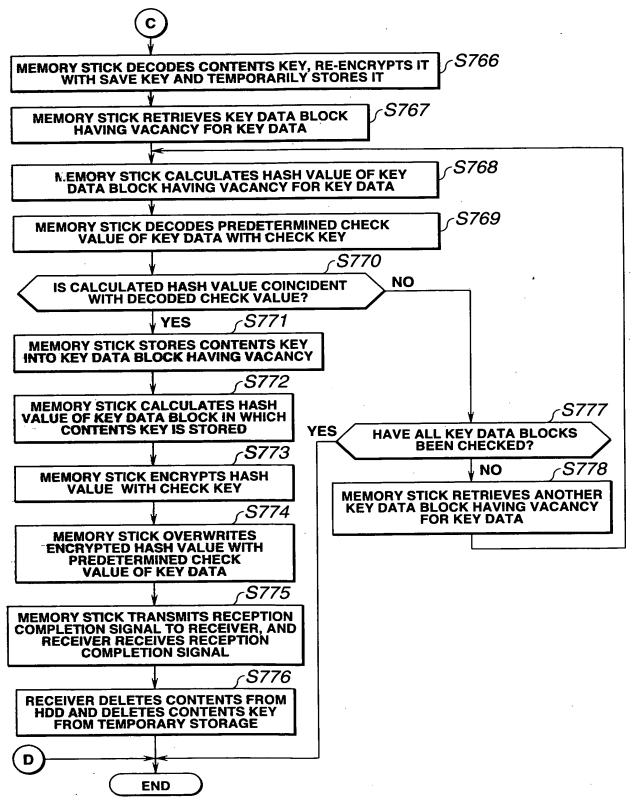
**FIG.80** 



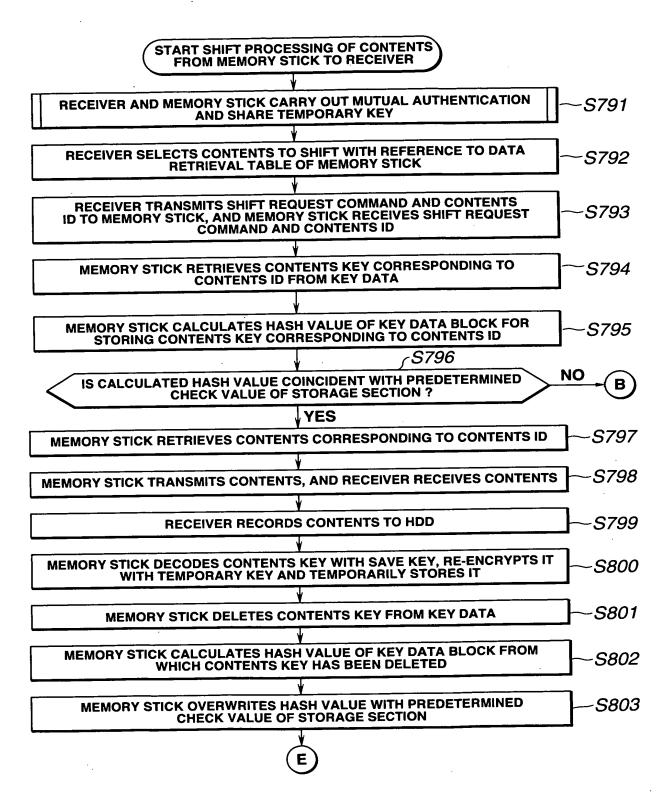
**FIG.81** 



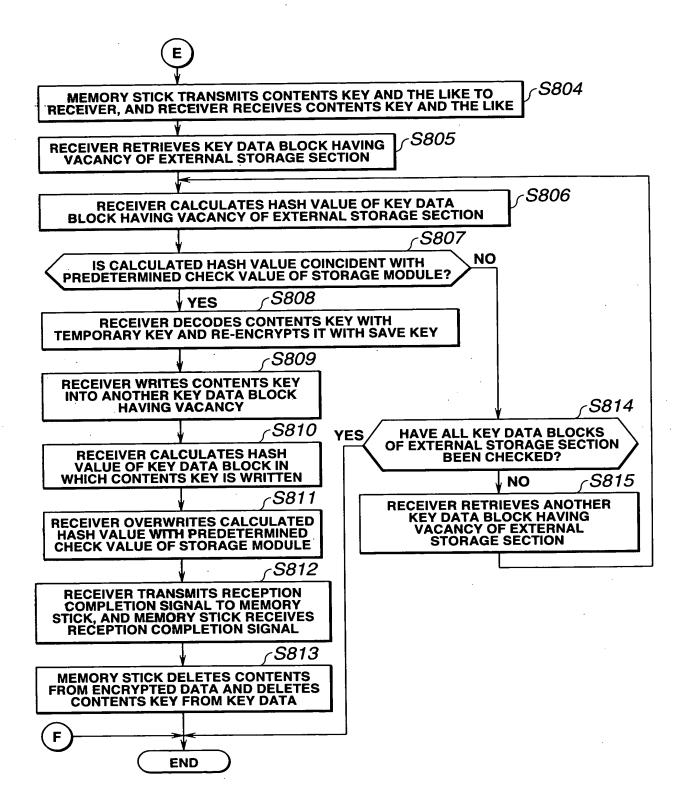
**FIG.82** 



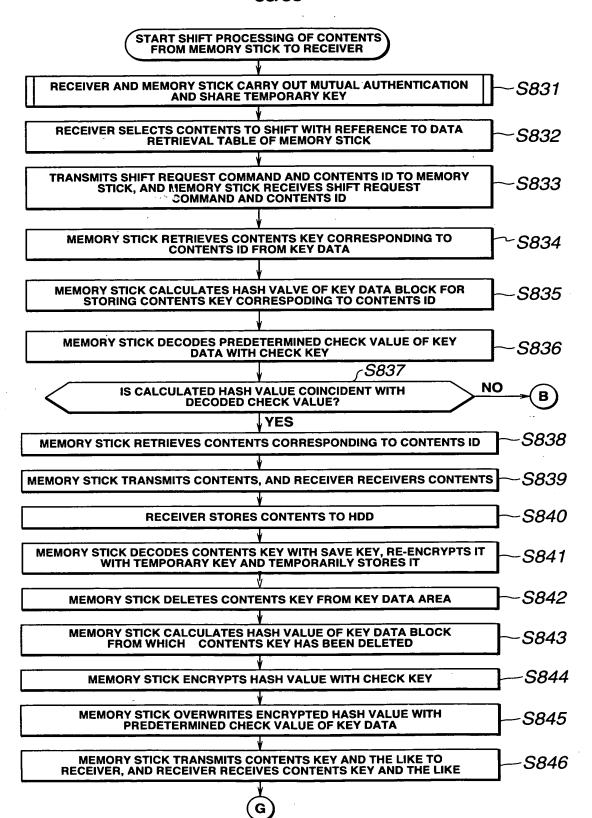
**FIG.83** 



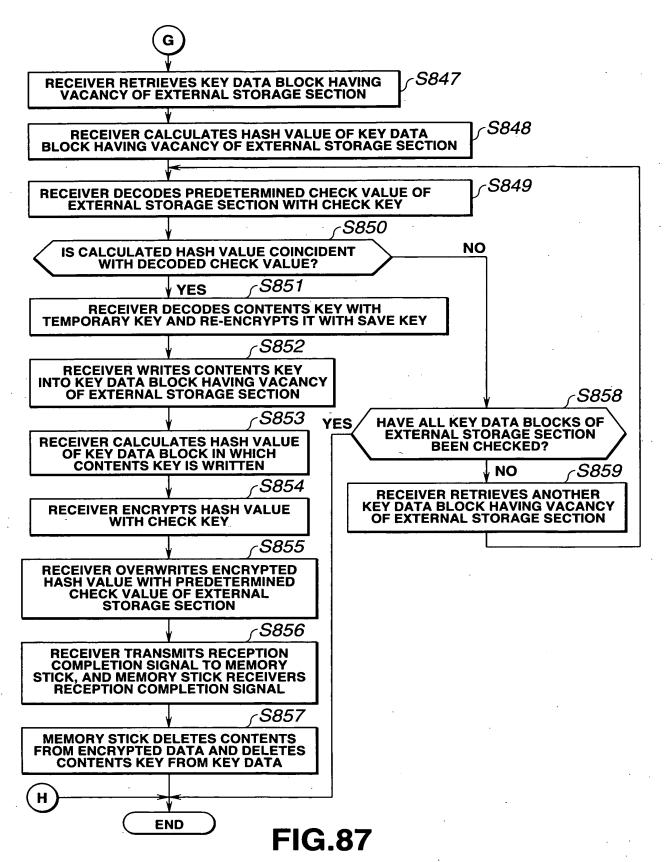
**FIG.84** 

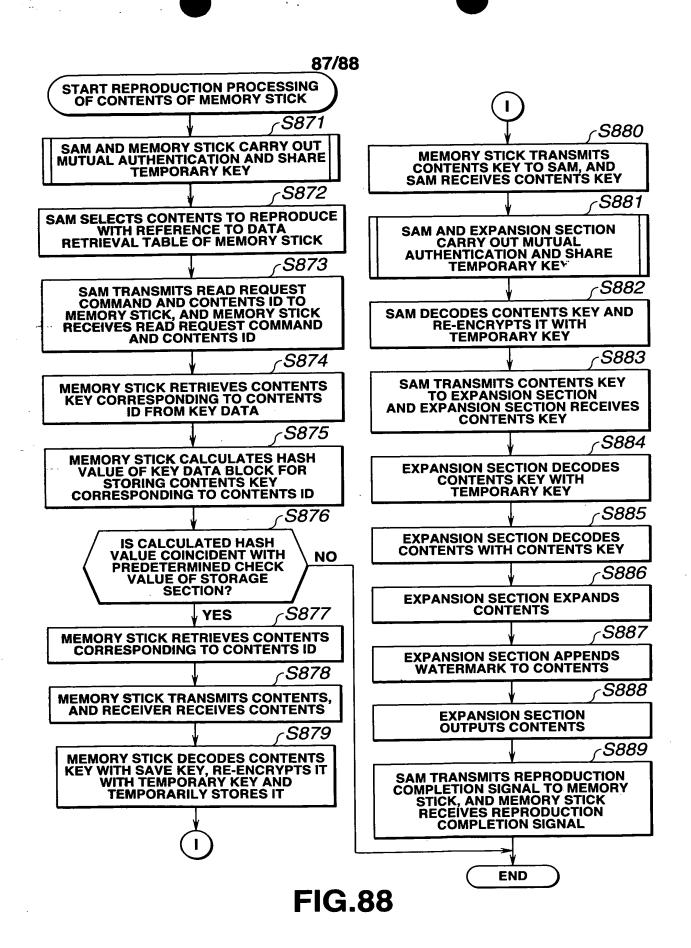


**FIG.85** 



**FIG.86** 





#### 88/88 START REPRODUCTION PROCESSING OF CONTENTS OF MEMORY STICK -S911 -S901 MEMORY STICK TRANSMITS CONTENTS KEY TO RECEIVER, AND RECEIVER RECEIVES SAM AND MEMORY STICK CARRY **OUT MURAL AUTHENTICATION AND** SHARE TEMPORARY KEY **CONTENTS KEY** ·S902 ~S912 SAM SELECTS CONTENTS TO REPRODUCE WITH REFERENCE TO DATA RETRIEVAL SAM AND EXPANSION SECTION CARRY OUT MUTUAL AUTHENTICATION AND SHARE TABLE OF MEMORY STICK <sup>.</sup>S903 TEMPORARY KEY ~S913 SAM TRANSMITS READ REQUEST COMMAND AND CONTENTS ID TO MEMORY STICK, AND MEMORY STICK RECEIVES READ REQUEST COMMAND SAM DECODES CONTENTS KEY AND **RE-ENCRYPTS IT WITH** AND CONTENTS ID **TEMPORARY KEY** ·S904 ∂S914 SAM TRANSMITS CONTENTS KEY MEMORY STICK RETRIEVES CONTENTS TO EXPANSION SECTION **KEY CORRESPONDING TO CONTENTS** AND EXPANSION SECTION RECEIVES **ID FROM KEY DATA CONTENTS KEY** ~S905 S915 MEMORY STICK CALCULATES HASH VALUE OF KEY DATA BLOCK FOR STORING CONTENTS KEY CORRESPONDING TO CONTENTS ID EXPANSION SECTION DECODES CONTENTS KEY WITH **TEMPORARY KEY** S916 S906 EXPANSION SECTION DECODES CONTENTS WITH CONTENTS KEY MEMORY STICK DECODES PREDETERMINED CHECK VALUE OF **KEY DATA WITH CHECK KEY** S917 -S907 **EXPANSION SECTION EXPANDS CONTENTS** IS CALCULATED HASH VALUE COINCIDENT WITH DECODED CHECK VALUE? NO S918 **EXPANSION SECTION APPENDS** YES ~S908 **WATERMARK TO CONTENTS** MEMORY STICK RETRIEVES CONTENTS CORRESPONDING TO CONTENTS ID ~S919 **EXPANSION SECTION** S909 **OUTPUTS CONTENTS** MEMORY STICK TRANSMITS CONTENTS, AND RECEIVER RECEIVES CONTENTS -S920 SAM TRANSMITS REPRODUCTION S910 COMPLETION SIGNAL TO MEMORY STICK, AND MEMORY STICK RECEIVES REPRODUCTION MEMORY STICK DECODES CONTENTS KEY WITH SAVE KEY, RE-ENCRYPTS IT WITH TEMPORARY KEY AND COMPLETION SIGNAL TEMPORARILY STORES IT **END FIG.89**